

普通高等教育“十一五”国家级规划教材

丛书主编　谭浩强

高等院校计算机应用技术规划教材

应用型教材系列

计算机安全技术

邵丽萍　编著

根据“中国高等院校计算机基础教育课程体系”组织编写

清华大学出版社

高等院校计算机应用技术规划教材——应用型教材系列
丛书主编　谭浩强

计算机安全技术

邵丽萍　编著

清华大学出版社
北　京

内 容 简 介

随着21世纪信息时代的到来，计算机技术和网络技术已深入到社会的各个领域，人类对计算机和网络的依赖越来越大，计算机安全问题已经成为全社会关注和讨论的焦点。本书针对这些问题，系统地介绍了几种常用的计算机安全技术，主要包括计算机实体安全技术、密码技术、软件安全技术、系统软件安全技术、计算机病毒防范技术、网络攻防技术、网络应用安全技术、运行安全技术等内容。

本书依据"提出问题→解决方法和技术→具体应用实例"的基本思路，采用案例引导、理论阐述、实例说明的编写方法，内容注重实用，结构清晰，图文并茂，通俗易懂，力求做到使读者在兴趣中学习计算机安全技术。本书既可作为高等院校、高职高专和计算机安全技术培训的使用教材，也可作为计算机安全技术爱好者的参考书。

图书在版编目（CIP）数据

计算机安全技术/邵丽萍编著. —北京：清华大学出版社，2012.10
（高等院校计算机应用技术规划教材——应用型教材系列）
ISBN 978-7-302-29371-2

Ⅰ. ①计…　Ⅱ. ①邵…　Ⅲ. ①计算机安全－高等学校－教材　Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2012)第158269号

责任编辑：谢　琛
封面设计：常雪影
责任校对：梁　毅
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：25.5　　**字　　数**：604千字
版　　次：2012年10月第1版　　**印　　次**：2012年10月第1次印刷
印　　数：1～4000
定　　价：39.00元

产品编号：048085-01

编辑委员会

《高等院校计算机应用技术规划教材》



《高等院校计算机应用技术规划教材》

进入21世纪，计算机成为人类常用的现代工具，每一个有文化的人都应当了解计算机，学会使用计算机来处理各种事务。

学习计算机知识有两种不同的方法：一种是侧重于理论知识的学习，从原理入手，注重理论和概念；另一种是侧重于应用的学习，从实际入手，注重掌握其应用的方法和技能。不同的人应根据其具体情况选择不同的学习方法。对多数人来说，计算机是作为一种工具来使用的，应当以应用为目的、以应用为出发点。对于应用型人才来说，显然应当采用后一种学习方法，根据当前和今后的需要，选择学习的内容，围绕应用进行学习。

学习计算机应用知识，并不排斥学习必要的基础理论知识，要处理好这两者的关系。在学习过程中，有两种不同的学习模型：一种是金字塔模型，亦称为建筑模型，强调基础宽厚，先系统学习理论知识，打好基础以后再联系实际应用；另一种是生物模型，植物并不是先长好树根再长树干，长好树干才长树冠，而是树根、树干和树冠同步生长的。对计算机应用型人才教育来说，应该采用生物模型，随着应用的发展，不断学习和扩展有关的理论知识，而不是孤立地、无目的地学习理论知识。

传统的理论课程采用以下的三部曲：提出概念—解释概念—举例说明，这适合前面第一种侧重于知识的学习方法。对于侧重于应用的学习者，我们提倡新的三部曲：提出问题—解决问题—归纳分析。传统的方法是：先理论后实际，先抽象后具体，先一般后个别。我们采用的方法是：从实际到理论，从具体到抽象，从个别到一般，从零散到系统。实践证明这种方法是行之有效的，减少了初学者在学习上的困难。这种教学方法更适合应用型人才。

检查学习好坏的标准，不是“知道不知道”，而是“会用不会用”，学习的目的主要在于应用。因此希望读者一定要重视实践环节，多上机练习，千万不要满足于“上课能听懂、教材能看懂”。有些问题，别人讲半天也不明白，自己一上机就清楚了。教材中有些实践性比较强的内容，不一定在课堂上由老师讲授，而可以指定学生通过上机掌握这些内容。这样做可以培养学生的自学能力，启发学生的求知欲望。

全国高等院校计算机基础教育研究会历来倡导计算机基础教育必须坚持面向应用的正确方向,要求构建以应用为中心的课程体系,大力推广新的教学三部曲,这是十分重要的指导思想,这些思想在“中国高等院校计算机基础课程”中做了充分的说明。本丛书完全符合并积极贯彻全国高等院校计算机基础教育研究会的指导思想,按照“中国高等院校计算机基础教育课程体系”组织编写。

这套“高等院校计算机应用技术规划教材”是根据广大应用型本科和高职高专院校的迫切需要而精心组织的,其中包括4个系列:

(1) 基础教材系列。该系列主要涵盖了计算机公共基础课程的教材。

(2) 应用型教材系列。适合作为培养应用型人才的本科院校和基础较好、要求较高的高职高专学校的主干教材。

(3) 实用技术教材系列。针对应用型院校和高职高专院校所需要掌握的技能技术编写的教材。

(4) 实训教材系列。应用型本科院校和高职高专院校都可以选用这类实训教材。其特点是侧重实践环节,通过实践(而不是通过理论讲授)去获取知识,掌握应用。这是教学改革的一个重要方面。

本套教材是从1999年开始出版的,根据教学的需要和读者的意见,几年来多次修改完善,选题不断扩展,内容日益丰富,先后出版了60多种教材和参考书,范围包括计算机专业和非计算机专业的教材和参考书;必修课教材、选修课教材和自学参考的教材。不同专业可以从中选择所需要的部分。

为了保证教材的质量,我们遴选了有丰富教学经验的高校优秀教师分别作为本丛书各教材的作者,这些老师长期从事计算机的教学工作,对应用型的教学特点有较多的研究和实践经验。由于指导思想明确,作者水平较高,教材针对性强,质量较高,本丛书问世7年来,愈来愈得到各校师生的欢迎和好评,至今已发行了240多万册,是国内应用型高校的主流教材之一。2006年被教育部评为普通高等教育“十一五”国家级规划教材,向全国推荐。

由于我国的计算机应用技术教育正在蓬勃发展,许多问题有待深入讨论,新的经验也会层出不穷,我们会根据需要不断丰富本丛书的内容,扩充丛书的选题,以满足各校教学的需要。

本丛书肯定会有不足之处,请专家和读者不吝指正。

全国高等院校计算机基础教育研究会会长
《高等院校计算机应用技术规划教材》主编　**谭浩强**

2008年5月1日于北京清华园



随着21世纪信息时代的到来，计算机技术得到了前所未有的发展与应用，信息技术和信息产业正在改变传统的生产、经营和生活方式，信息已成为社会发展的重要战略资源。电子商务、电子政务、电子税务、电子银行、电子海关、电子证券、网络书店、网上拍卖、网上购物、网上交易等计算机应用系统在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。随着人类对计算机和计算机网络的依赖越来越大，计算机安全问题逐渐成为全社会关注和讨论的焦点。

为了解决计算机安全的实际问题，针对社会对计算机安全技术的迫切需求，各高等院校开始注重计算机安全方面的课题研究，并在相关专业相继开设了计算机安全方面的课程。撰写本书的主要目的，是帮助学生与读者理解计算机安全技术的基本原理和基本思想，更快地掌握计算机安全的技术与工具，帮助老师进行计算机安全技术教学。

作为一本教材，本书对内容做了精心设计和安排，在内容的编排上体现了新的计算机教学思想和方法，以“案例引导提出问题→解题方法和技术→应用实例具体说明→案例讨论归纳总结”的基本思路来介绍计算机安全技术。本着“理论方法知道，技术工具会用”的原则，将计算机安全分为物理安全、软件安全、网络安全和运行安全4部分，从计算机安全基础知识、计算机硬件与基础设施安全、密码技术、软件安全技术、系统安全技术、计算机病毒防治技术、网络攻防技术、网络应用安全技术和应急响应与灾难恢复等方面来组织编写。

本书具有如下特色：

1. 内容全面、结构清晰

本书对整个内容做了精心设计和安排，全书分为4个方面：实体安全，软件安全，网络安全与运行安全。由硬到软，从网络到应用，首先概要介绍计算机安全的基本内容，然后分章介绍实体安全技术、密码技术、软件安全技术、系统软件安全技术，计算机病毒防治技术，网络攻防技术，网络应用安全技术，最后介绍计算机系统运行过程中的应急响应与灾难恢复。

2. 案例贯穿，由始至终

对每一章的内容也做了统一规划与要求，每章开头提出“学习目标”，并通过一个“引导案例”指出本章研究领域存在的安全危害案例，然后分析计算机安全某方面存在的威胁，再介绍保护计算机安全的技术与方法措施，最后通过

一个或多个“案例讨论”，归纳总结问题，达到进一步提高所学内容的目的。

3. 理论实践，紧密结合

在使用本书学习时，可结合每章的具体应用实例，上机实践，按照书中的操作步骤，在短时间内掌握所介绍的计算机安全技术或工具的使用方法，实现保护计算机安全的目标，进一步理解计算机安全技术的理论知识。

4. 通俗易懂、好学好用

本书文字通俗易懂，本着复杂问题简单化的原则介绍理论与概念，尽量通过实例与图形来说明问题，使学生与读者更容易理解计算机安全技术的基本思想和方法技巧。

全书分为 9 章，主要包括以下内容：

第 1 章介绍计算机安全的基本概念、计算机安全面临的威胁、保护计算机安全涉及的技术，保护计算机安全的基本原则与措施。通过本章的学习，使读者对计算机安全有一个整体的认识。

第 2 章通过对硬件安全、基础设施安全、环境安全、设备安全、电源系统安全以及通信线路安全的详细介绍，帮助读者了解计算机物理安全的相关知识，并且能够运用本章介绍的知识和技术来维护计算机系统的物理安全。

第 3 章介绍常用密码学、加密算法的基本概念、破解密码的方法及密码技术的应用，通过具体实例说明文件加密的方法与用户密码的使用技巧，加深读者对密码技术方面的理解，使读者能够运用一些工具软件来保护自己在工作或生活中的机密或隐私数据。

第 4 章介绍软件加密技术、软件分析技术、软件加壳与脱壳技术、软件防盗版技术以及常用的软件保护方法，通过应用实例介绍了如何对软件进行加壳与脱壳，如何通过压缩方法保护软件的安全，如何对 PDF、Excel 文件进行加密与解密。

第 5 章介绍系统软件的重要性与系统软件面临的安全威胁，具体介绍了 Windows 操作系统与 Linux 操作系统的安全管理，并介绍了 Access 数据库系统、SQL Server 数据库系统与 Oracle 数据库系统的安全配置。通过本章的学习，使读者了解操作系统与数据库系统安全的多个方面，从而提高读者安全使用操作系统与数据库系统的水平。

第 6 章介绍计算机病毒的定义与危害，具体介绍了传统的计算机病毒与互联网下的病毒的特点与清除方法，系统介绍了防治计算机病毒采用的预防、检测与清除方法，通过应用实例介绍了清除脚本病毒的方法、防治 U 盘病毒的方法、染毒计算机数据恢复的方法以及使用 360 安全卫士预防查杀病毒的方法。

第 7 章从网络攻击与防御两个角度进行阐述，介绍网络攻击的概念、使用的手段与工具，具体介绍了防范端口与漏洞扫描、缓冲区溢出攻击及其防范、ARP 欺骗、DoS 与 DDoS 攻击检测与防御、防火墙技术、入侵检测技术以及蜜罐技术，通过应用实例的介绍，加深读者对网络安全和攻防方面的基础知识和技术的理解，提高读者应对网络攻击的能力。

第 8 章从网络应用安全的角度进行阐述，介绍网络应用存在的安全威胁与保护网络应用安全应该采取的防范措施，具体介绍了防范口令安全、Email 安全、QQ 聊天安全、网上购物安全、网上银行与网上支付安全应该采取的具体措施。

第 9 章从运行安全的角度进行阐述，介绍计算机信息系统在遇到紧急安全事件时应该采取的应急响应措施与操作流程，具体介绍了作为应急响应与灾难恢复的基础数据备份的技术，详细介绍了灾难恢复指标、等级、资源与应该采取的策略，并介绍了容灾建设的原则、指导思想与计划，同时介绍了处于研究发展之中的容错技术与容错系统，并通过应用实例介绍了如何使用 Ghost 进行文件备份与还原，如何运用 Windows 7 创建系统映像。

通过学习与使用本书能够带领学生与读者走进学习计算机安全技术的大门，计算机安全技术在飞速发展，新技术、新产品与新工具会越来越多，本书主要着眼于培养学生与读者具有计算机安全的意识与基本思想，通过学习本书的理论知识，按照本书介绍的应用实例与安全防范措施上机上网操作实践，可以使学生与读者尽快了解计算机安全技术的基础理论，掌握保护计算机安全的基本技术与基本方法。

本书由邵丽萍统一编写提纲及统稿，并编写了第 1、第 3 章，第 4、第 5 章由张后扬编写，第 9 章由吕希艳编写，第 2 章由崔卫平编写，第 6 章由张驰编写，第 7 章由史晓丹编写，第 8 章由廖梦翔编写，李竹行、沈泽军、喻晔、肖维斯、王黛也参与了本书的编写工作。

本书有教师配套使用的电子课件，由出版社提供给使用本教材的授课老师。

作　者

2012 年 6 月


目录



第1章 计算机安全概述

学习目标

通过本章的学习，能够——

- 了解计算机安全的概念；
- 了解计算机安全面临的威胁；
- 知道保护计算机安全的基本原则与措施；
- 知道对计算机安全进行评估的标准。

引导案例

计算机已经成为人们进行事务处理、科学研究与学习的有力工具，并给人们的日常生活带来各种便利和快捷，人们利用计算机进行办公、计算数据、召开会议、购买商品、通信与教育等。但是，就在人们享受计算机带来的进步与惊喜，并依赖计算机帮助的今天，你可曾想到计算机并不安全？

2011年1月13日，厦门易名的DNS服务器遭受大规模转嫁拒绝服务攻击（原目标：网游私服），导致无法提供正常的解析服务约4小时。5月6日，江苏联通业务门户网站遭受来自手机用户的拒绝服务攻击；根据CNCERT（国家计算机网络应急技术处理协调中心）的监测和江苏联通的分析发现，这些手机均被感染"毒媒"病毒。6月28日新浪发现微博跨站漏洞，受此漏洞影响的用户超过7万。8月18日和19日，新疆电信DNS服务器两次遭遇来自网内的伪造源IP攻击。9月5日约18:30至18:50，全网DNS流量（出向）出现异常，但未对互联网造成影响。事件原因是攻击者发起了指向国外IP地址且伪造源IP的攻击。

2011年1月至9月中国大陆有近3.1万个网站被黑客篡改，其中被篡改的政府网站为2312个。在此期间，CNCERT对国务院部门门户网站进行了网络安全常规检查，约有55%的部门或网站存在安全风险，共发现548万余个境内主机IP地址感染了木马或僵尸程序。

2010年1月12日上午，全球最大的中文搜索引擎百度遭受攻击，出现大规模无法访问的状况，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。这次

百度大面积故障时间长达5个小时，也是百度自2006年9月以来发生的最大一次严重断网事故，在国内外互联网界造成了重大影响。

2009年9月，全国被恶意篡改的网站数量为3513个，其中政府网站(.gov.cn)被篡改的数量为256个；国家计算机网络应急技术处理协调中心检测到国内外被控制的僵尸网络客户端共14万多个，其中超过半数位于中国大陆；全国与互联网相连的网络管理中心有95%都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。

2008年，一个全球性的黑客组织，利用欺诈程序在一夜之间从世界49个城市的银行的ATM机中盗走了900万美元。

2007年，俄罗斯黑客成功劫持Windows Update下载服务器。

2006年9月13日，百度承认遭受"大规模的不明身份黑客的攻击"，导致百度搜索服务在中国各地出现了近30分钟的故障。

2002年，英国著名黑客加里·麦金农被指控侵入美国军方90多个计算机系统，造成约140万美元的损失，美方称此案为史上"最大规模入侵军方网络事件"。2009年，英国法院裁定准许美方引渡麦金农。

2001年，中美撞机事件发生后，中美黑客之间发生的网络大战愈演愈烈。自4月4日以来，美国黑客组织PoizonBOx不断袭击中国网站。对此，我国的网络安全人员积极防备美方黑客的攻击。中国一些黑客组织则在"五一"期间打响了"黑客反击战"。

2000年1月，日本政府11个省、厅受到黑客攻击。总务厅的统计信息全部被删除；外务省主页3分钟内遭到攻击1000余次；日本最高法院主页两天内遭受攻击3000余次。日本政府立即成立反黑特别委员会，拨款24亿日元研究入侵检测技术、追踪技术、病毒技术和密码技术。

2000年2月7日发生攻击美国知名网站案件：损失12亿美元，影响百万网民，Yahoo、Amazon、CNN、Buy、eBay、E-Trade等均受影响。

1998年，为了获得在洛杉矶地区Kiss-FM电台第102个呼入者的奖励——保时捷跑车，Kevin Poulsen控制了整个地区的电话系统，以确保他是第102个呼入者。最终，他如愿以偿地获得了跑车并为此入狱三年。

美国因网络安全问题造成直接经济损失170亿美元/年。

美国金融界因计算机犯罪造成损失100亿美元/年。

由此可见，计算机安全涉及国家、个人的信息安全甚至财产安全等多个方面。因此，计算机安全，以及相关的计算机安全技术应受到人们的重视，提高计算机安全防护意识，强化计算机安全已经成为当务之急。

1.1 什么是计算机安全

随着21世纪信息时代的到来，计算机技术得到了前所未有的发展与应用，社会对计算机系统的依赖日益增强，网络已经成为社会发展的重要保证。在计算机应用日益广泛和深入的同时，计算机安全问题也变得日益复杂和突出，网络的脆弱性和复杂性增加了威胁和攻击的可能性。如何保护企业与个人计算机的安全，成为信息时代企业与个人面临的实际

问题。

本节将介绍计算机安全的定义、属性与计算机安全的范畴。

1.1.1 计算机安全的定义

1. 计算机安全定义

要清楚什么是计算机安全，首先要知道安全的含义。什么是安全呢？

计算机安全技术专家 Bruce Schneier 曾经说过这样一段话："如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏；相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全。"

根据国际标准化组织（ISO）的定义，计算机安全指为数据处理系统建立的技术和管理上的安全保护，确保计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。

该定义包含了两方面的内容：物理安全和逻辑安全。物理安全指计算机系统设备及相关设备受到保护，免于被破坏、丢失等；逻辑安全指保障计算机系统的安全，即保障计算机中所处理的信息的完整性、保密性和可用性。

从此定义可以看到计算机安全就是计算机资源的安全。计算机资源包括系统资源（软件、硬件，配套设施，文件资料等）；信息资源（计算机系统所处理、存储和传输的各类数据与信息）。

从此定义还可以看出，保护计算机安全就是保护计算机系统的安全。计算机系统是由计算机及其相关的配套设备、设施（含网络）构成，具有采集、接收、加工、存储、传输、检索、按程序快速计算和判断并输出处理结果等功能的人机系统，简单地说就是进行数据处理的系统。

2. 计算机安全目标

计算机安全的目标是使全部计算机系统资源保持正常状态。包括：

（1）硬件设备及有关设施运转正常；

（2）系统服务正常；

（3）各种系统软件及所需的应用软件（包括相关文档）完整、齐全；

（4）系统的信息资源完整、有效，不被非法使用。

3. 计算机系统的安全性问题

计算机安全不仅涉及计算机系统本身的技术问题、管理问题，还涉及法学、犯罪学、心理学的问题；其内容包括了计算机安全理论与策略，计算机安全技术、安全管理、安全评价、安全产品以及计算机犯罪与侦察、计算机安全法律、安全监察等。

概括起来，计算机系统的安全性问题可分为三大类，即技术安全类、管理安全类和政

策法律类。

技术安全是指计算机系统中采用具有一定安全性的硬件、软件来实现对计算机系统及其所存数据的安全保护，当计算机系统受到无意或恶意的攻击时仍能保证系统正常运行，保证系统内的数据不增加、不丢失，不泄露。

管理安全是指诸如软硬件意外故障、场地的意外事故、管理不善导致的计算机设备和数据介质的物理破坏、丢失等安全问题。

政策法律类是指政府部门建立的有关计算机犯罪、数据安全保密的法律道德准则和政策法规、法令，本书主要讨论技术安全，泛指计算机安全技术。

1.1.2 计算机安全的属性

在美国国家信息基础设施（NII）的文献中，给出了计算机安全的五个属性：可用性、可靠性、完整性、保密性和不可抵赖性。这五个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛领域。这五个属性的定义如下：

1. 可用性（availability）

可用性是指得到授权的实体在需要时可访问资源和服务。也就是说，无论何时，只要用户需要，信息系统必须是可用的，也就是说信息系统不能拒绝服务。网络系统最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的，多方面的（语音、数据、文字和图像等），有时还要求时效性。网络系统必须随时满足用户通信的要求。

攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

2. 可靠性（reliability）

可靠性是指系统在规定条件下和规定时间内、完成规定功能的概率。可靠性是计算机系统安全最基本的要求之一，系统不可靠，事故不断，也就谈不上系统的安全。目前，对于系统可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备，采取合理的冗余备份措施仍是最基本的可靠性对策，然而，有许多故障和事故，则与软件可靠性、人员可靠性和环境可靠性有关。

3. 完整性（integrity）

完整性是指计算机系统的信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改。即信息的内容不能为未授权的第三方修改。信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等。

4. 保密性（confidentiality）

保密性是指确保计算机系统的信息不暴露给未授权的实体或进程。即信息的内容不

会被未授权的第三方所知。这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人私密（如浏览习惯、购物习惯）。防止信息失窃和泄露的保障技术称为保密技术。

5. 不可抵赖性（non-Repudiation）

不可抵赖性也称作不可否认性。不可抵赖性是面向通信双方（人、实体或进程）信息真实同一的安全要求，它包括收、发双方均不可抵赖。一是源发证明，它提供给信息接收者以证据，这将使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；二是交付证明，它提供给信息发送者以证明这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

1.1.3 计算机安全范畴

计算机安全范畴涉及实体安全、运行安全、信息安全与网络安全四个方面。

1. 实体安全

计算机系统的实体安全是整个计算机系统安全的前提。因此，保证实体的安全是十分重要的。计算机系统的实体安全是指计算机系统硬件设备及相关设施的安全、正常运行，具体内容包括以下三个方面：

（1）环境安全。

环境安全是指计算机和信息系统的设备及其相关设施所放置的机房的地理环境、气候条件、污染状况以及电磁干扰等对实体安全的影响。

（2）设备安全。

设备安全保护是指计算机信息系统的设备及相关设施的防盗、防毁以及抗电磁干扰、静电保护、电源保护等几个方面。

（3）媒体安全。

媒体安全是指对存储有数据的媒体进行安全保护。存储信息的媒体主要有：纸介质、磁介质（硬盘、软盘、磁带）、半导体介质的存储器以及光盘。媒体是信息和数据的载体，媒体损坏、被盗或丢失，损失最大的不是媒体本身，而是媒体中存储的数据和信息。对于存储有一般数据信息的媒体，这种损失在没有备份的情况下会造成大量人力和时间的浪费，对于存储有重要和机密信息的媒体，造成的是无法挽回的巨大损失，甚至会影响到社会的安定和战争的成败。媒体的安全保护，一是控制媒体存放的环境要满足要求，对磁介质媒体库房温度应控制在15℃～25℃之间，相对湿度应控制在45％～65％之间，否则易发生霉变，造成数据无法读出。二是完善相应管理制度，存储有数据和信息的媒体应有专人管理，使用和借出应有十分严格的控制。对于需要长期保存的媒体，则应定期翻录，避免因介质老化而造成损失。

2. 运行安全

运行安全的保护是指计算机信息系统在运行过程中的安全必须得到保证，使之能对

信息和数据进行正确的处理，正常发挥系统的各项功能。影响运行安全主要有下列因素。

(1) 工作人员的误操作。

工作人员的业务技术水平、工作态度及操作流程的不合理都会造成误操作，误操作带来的损失可能是难于估量的。常见的误操作有：误删除程序和数据、误移动程序和数据的存储位置、误切断电源以及误修改系统的参数等。

(2) 硬件故障。

造成硬件故障的原因很多，如电路中的设计错误或漏洞、元器件的质量、印刷电路板的生产工艺、焊接的工艺、供电系统的质量、静电影响及电磁场干扰等，均会导致在运行过程中硬件发生故障。硬件故障，轻则使计算机信息系统运行不正常、数据处理出错，重则导致系统完全不能工作，造成不可估量的巨大损失。

(3) 软件故障。

软件故障通常是由于程序编制错误而引起的。随着程序的加大，出现错误的地方就会越来越多。这些错误对于很大的程序来说是不可能完全排除的，因为在对程序进行调试时，不可能通过所有的硬件环境和处理数据。这些错误只有当满足它的条件时才会表现出来，平时是不能发现的。众所周知，微软的 Windows 95、Windows 98 均存在几十处程序错误，发现这些错误后均通过打补丁的形式来解决，以至于“打补丁”这个词在软件产业界已经习以为常。程序编制中的错误尽管不是恶意的，但仍会带来巨大的损失。

(4) 计算机病毒。

计算机病毒是破坏计算机信息系统运行安全的最重要因素之一，轻则影响计算机运行速度，使计算机不能正常运行，重则使计算机处于瘫痪状态，给用户带来不可估量的损失。Internet 在为人们提供信息传输和浏览方便的同时，也为计算机病毒的传播提供了方便，例如，1999 年 4 月 26 日，全球便遭到了最厉害的病毒 CIH 的洗劫，全球 6000 万台计算机被破坏，它不但破坏 BIOS 芯片，而且破坏硬盘中的数据，所造成的损失难以用金钱的数额来估计。

(5) “黑客”攻击。

“黑客”具有高超的技术，对计算机硬、软件系统的安全漏洞非常了解。他们的攻击目的具有多样性，一些是恶意的犯罪行为，一些是玩笑型的调侃行为，也有一些是正义的攻击行为，如在美国等北约国家对南联盟轰炸期间，许多黑客对美国官方网站进行攻击，他们的目的是反对侵略战争和霸权主义。随着 Internet 的发展和普及，黑客的攻击会越来越多。

(6) 恶意破坏。

恶意破坏是一种犯罪行为，它包括对计算机信息系统的物理破坏和逻辑破坏两个方面。物理破坏，只要犯罪分子能足够地接近计算机便可实施，通过暴力对实体进行毁坏。逻辑破坏，是利用冒充身份、窃取口令等方式进入计算机信息系统，改变系统参数、修改有用数据、修改程序等，造成系统不能正常运行。物理破坏容易发现，而逻辑破坏具有较强的隐蔽性，常常不能及时发现。

(7) 自然灾害。

3. 信息安全

信息安全是指防止信息财产被故意地或偶然地泄露、破坏、更改，保证信息使用完整、有效、合法。信息安全的破坏主要表现在如下几个方面。

(1) 信息可用性遭到破坏。

信息的可用性是指用户的应用程序能够利用相应的信息进行正确的处理。计算机程序与信息数据文件之间都有约定的存放磁盘、文件夹、文件名的关系，如果将某数据文件的文件名称进行了改变，对于它的处理程序来说，这个数据文件就变成了不可用，因为它不能找到要处理的文件。同样，将数据文件存放的磁盘或文件夹进行改变后，数据文件的可用性也遭了破坏。另一种情况是在数据文件中加入一些错误的或应用程序不能识别的信息代码，导致程序不能正常运行或得到错误的结果。

(2) 对信息完整性的破坏。

信息的完整性包含信息数据的多少、正确与否、排列顺序等几个方面。任何一个方面遭破坏，均会破坏信息的完整性。信息完整性的破坏可能来自多个方面，人为因素、设备因素、自然因素及计算机病毒等，均可能破坏信息的完整性。

(3) 保密性的破坏。

对保密性的破坏一般包括非法访问、信息泄露、非法拷贝、盗窃以及非法监视、监听等方面。非法访问指盗用别人的口令或密码等对超出自己权限的信息进行访问、查询、浏览。信息泄露包含人为泄露和设备、通信线路的泄露。

人为泄露是指掌握有机密信息的人员有意或无意地将机密信息传给了非授权的人员。设备及通信线路的信息泄露主要指电磁辐射泄露、搭线侦听、废物利用几个方面。电磁辐射泄露，主要是指计算机及其设备、通信线路及设备在工作时所产生的电磁辐射，利用专门的接收设备就可以在很远的地方接收到这些辐射信息。

4. 网络安全

计算机网络是把具有独立功能的多个计算机系统通过通信设备和通信信道连接起来，并通过网络软件（网络协议、信息交换方式及网络操作系统）实现网络中各种资源的共享。

网络从覆盖的地域范围的大小可分为局域网、区域网及广域网。从完成的功能上看，网络由资源子网和通信子网组成。对于计算机网络的安全来说，它主要包括两个部分，一是资源子网中各计算机系统的安全性；二是通信子网中的通信设备和通信线路的安全性。对它们安全性的威胁主要有以下几种形式。

(1) 计算机犯罪行为。

计算机犯罪行为包括故意破坏网络中计算机系统的硬软件系统、网络通信设施及通信线路；非法窃听或获取通信信道中传输的信息；假冒合法用户非法访问或占用网络中的各种资源；故意修改或删除网络中的有用数据等。

(2) 自然因素的影响。

自然因素的影响包括自然环境和自然灾害的影响。自然环境的影响包括地理环境、

气候状况、环境污染状况及电磁干扰等多个方面。自然灾害有地震、水灾、大风、雷电等，它们可能给计算机网络带来致命的危害。

(3) 计算机病毒的影响。

现今网络是计算机病毒最主要的传播方式，病毒可以对计算机用户的数据与信息进行窃取与破坏，会造成网络运行速度下降，甚至导致整个网络系统瘫痪。

(4) 人为失误和事故的影响。

人为失误是非故意的，但它仍会给计算机网络安全带来巨大的威胁。例如，某网络管理人员违章带电拔插网络服务器中的板卡，导致服务器不能工作，使整个网络瘫痪，这期间可能丢失了许多重要的信息，延误了信息的交换和处理，其损失可能是难以弥补的。网络越大，其安全问题就越是突出，安全保障的困难也就越大。近年来，随着计算机网络技术的飞速发展和应用的普及，国际互联网的用户大幅度增加。就我国而言，目前已有1000万用户接入国际互联网，人们在享受互联网给工作、生活、学习带来各种便利的同时，也承受了因网络安全性不足而造成的诸多损失。国际互联网本身就是在没有政府的干预和指导下无序发展起来的。它过分强调了开放性和公平性，而忽略了安全性。网络中每个用户的地位均是同等的，网络中没有任何人是管理者。近年来，互联网上黑客横行、病毒猖獗、有害数据泛滥、犯罪事件不断发生，暴露了众多的安全问题，引起了各国政府的高度重视。

1.2 计算机安全威胁

计算机、网络在给人们生活与工作带来巨大便利的同时，也给人们带来了极大的风险和挑战。计算机技术迅猛发展的同时，也面临各种各样的威胁，本节主要介绍计算机系统由于自身的脆弱性、外来的攻击与威胁和计算机犯罪带来的安全威胁。

1.2.1 计算机系统自身的脆弱性

1. 硬件的脆弱性

(1) 计算机系统的硬件均需要提供满足要求的电源才能正常工作，一旦切断电源，哪怕是极其短暂的一刻，计算机系统的工作也会被间断。

(2) 计算机是利用电信号对数据进行运算和处理。因此，环境中的电磁干扰能引起处理错误，得出错误的结论，并且所产生的电磁辐射会产生信息泄露。

(3) 电路板焊点过分密集，极易产生短路而烧毁器件。接插部件多，接触不良的故障时有发生。

(4) 体积小、重量轻、物理强度差，极易被偷盗或毁坏。

(5) 电路高度复杂，设计缺陷在所难免，加上有些不怀好意的制造商还故意留有“后门”。

2. 操作系统的脆弱性

任何应用软件均是在操作系统的支持下执行的，操作系统的不安全是计算机系统不

安全的重要原因。操作系统的脆弱性表现在以下几个方面。

(1) 操作系统的程序可以动态链接。这种方式虽然为软件开发商进行版本升级时提供了方便,但“黑客”也可以利用此法攻击系统或链接计算机病毒程序。

(2) 操作系统支持网上远程加载程序,这为实施远程攻击提供了技术支持。

(3) 操作系统通常提供 DEMO 软件,这种软件在 UNIX、Windows NT 操作系统上与其他系统核心软件具有同等的权力。借此摧毁操作系统十分便捷。

(4) 系统提供了 Debug 与 Wizard,它们可以将执行程序进行反汇编,方便地追踪执行过程。掌握好了这两项技术,几乎可以做“黑客”的所有事情。

(5) 操作系统的设计缺陷。“黑客”正是利用这些缺陷对操作系统进行致命攻击。

3. 数据库管理系统的脆弱性

数据库管理系统中的核心是数据。存储数据的媒体决定了它易于修改、删除和替代。开发数据库管理系统的基本出发点是为了共享数据,而这又带来了访问控制中的不安全因素,在对数据进入访问时一般采用的是密码或身份验证机制,这些很容易被盗窃、破译或冒充。

4. 计算机网络的脆弱性

ISO 7498 网络协议形成时,基本上没有顾及安全的问题,只是后来才加进了 5 种安全服务和 8 种安全机制。国际互联网中的 TCP/IP 同样存在类似的问题。首先,IP 协议对来自物理层的数据包没有进行发送顺序和内容正确与否的确认。其次,TCP 通常总是默认数据包的源地址是有效的,这给冒名顶替带来了机会;与 TCP 位于同一层的 UDP 对包顺序的错误不作修改,对丢失包也不重传,因此极易受到欺骗。

5. 存储系统的脆弱性

存储系统分为内存和外存。

内存分为 RAM 和 ROM;外存有硬盘、软盘、磁带和光盘等。它们的脆弱性表现在如下几个方面。

(1) RAM 中存放的信息一旦掉电即刻丢失,并且易于在其内嵌入病毒代码。

(2) 硬盘构成复杂。既有动力装置,也有电子电路及磁介质,任何一部分出现故障均导致硬盘不能使用,丢失其内大量软件和数据。

(3) 软盘及磁带易损坏。它们的长期保存对环境要求高,保存不妥,便会发生霉变现象,导致数据不能读出。此外,盘片极易遭到物理损伤(折叠、划痕、破碎等),从而丢失其内程序和数据。

(4) 光盘盘片没有附在一起的保护封套,在进行数据读取和取放的过程中容易因摩擦而产生划痕,引起读取数据失败。此外,盘片在物理上脆性较大,易破碎而损坏,导致全盘上的数据丢失。

(5) 各种信息存储媒体的存储密度高,体积小,且重量轻,一旦被盗窃或损坏,损失巨大。

(6) 存储在各媒体中的数据均具有可访问性，数据信息很容易地被复制而不留任何痕迹。一台远程终端上的用户，可以通过计算机网络连接到你的计算机上，利用一些技术手段，访问到你系统中的所有数据，并按其目的进行复制、删除和破坏。

6. 信息传输中的脆弱性

(1) 信息传输所用的通信线路易遭破坏。

通信线路从铺设方式上分为架空明线和地埋线缆两种，其中架空明线更易遭到破坏。一些不法分子，为了贪图钱财，割掉通信线缆作为废金属卖掉，造成信息传输中断。自然灾害也易造成架空线缆的损坏，如大风、雷电、地震等。地埋线缆的损坏，主要来自人为的因素，各种工程在进行地基处理、深挖沟池、地质钻探等施工时，易损坏其下埋设的通信线缆。当然，发生塌方、砾石流等地质灾害时，其间的地埋线缆也定会遭到破坏。

(2) 线路电磁辐射引起信息泄露。

市话线路、长途架空明线以及短波、超短波、微波和卫星等无线通信设备都具有相当强的电磁辐射，可通过接收这些电磁辐射来截获信息。

(3) 架空明线易于直接搭线侦听。

(4) 无线信道易遭到电子干扰。

无线通信是以大气为信息传输媒体，发射信息时，都将其调制到规定的频率上，当另有一台发射机发射相同或相近频率的电磁波时，两个信号进行了叠加，使接收方无法正确接收信息。

1.2.2 计算机系统外来的攻击与威胁

计算机系统外来的安全威胁，大体上可以分为两种：一种是实体的攻击与威胁，另一种是信息的攻击与威胁。计算机犯罪和计算机病毒则包括了计算机系统实体和信息两方面的攻击与威胁。

1. 实体的攻击与威胁

实体的攻击与威胁主要指对计算机及其外部设备和网络的攻击与威胁，如各种自然灾害、人为破坏、设备故障、电磁干扰、战争破坏以及各种媒体的被盗和丢失等。对实体的威胁和攻击，不仅会造成国家财产的重大损失，而且会使系统的机密信息严重破坏和泄露。因此，对系统实体的保护是防止对信息威胁和攻击的首要一步，也是防止对信息威胁和攻击的天然屏障。

2. 信息的攻击与威胁

信息的攻击与威胁主要有两种，即信息泄露和信息破坏。

(1) 信息泄露是指偶然地或故意地获得(侦收、截获、窃取或分析破译)目标系统中的信息，特别是敏感信息，造成泄露事件。

(2) 信息破坏是指由于偶然事故或人为破坏，使信息的正确性、完整性和可用性受到破坏，如系统的信息被修改、删除、添加、伪造或非法复制，造成大量信息的破坏、修改或

丢失。

对信息进行人为的故意破坏或窃取称为攻击。根据攻击的方法不同,可分为被动攻击和主动攻击两类。

① 被动攻击。

被动攻击是指一切窃密的攻击。它是在不干扰系统正常工作的情况下进行侦收、截获、窃取系统信息,以便破译分析;利用观察信息、控制信息的内容来获得目标系统的位置、身份;利用研究机密信息的长度和传递的频度获得信息的性质。被动攻击不容易被用户察觉出来,因此它的攻击持续性和危害性都很大。

被动攻击的主要方法有:直接侦收、截获信息、合法窃取、破译分析以及从遗弃的媒体中分析获取信息。

② 主动攻击。

主动攻击是指篡改信息的攻击。它不仅能窃密,而且威胁到信息的完整性和可靠性。它是以各种各样的方式,有选择地修改、删除、添加、伪造和重排信息内容,造成信息破坏。

主动攻击的主要方式有:窃取并干扰通信线中的信息、返回渗透、线间插入、非法冒充以及系统人员的窃密和毁坏系统信息的活动等。

3. 计算机犯罪

计算机犯罪是利用暴力和非暴力形式,故意泄露或破坏系统中的机密信息,以及危害系统实体和信息安全的不法行为。暴力形式是对计算机设备和设施进行物理破坏,如使用武器摧毁计算机设备,炸毁计算机中心建筑等。而非暴力形式是利用计算机技术知识及其他技术进行犯罪活动,它通常采用下列技术手段:线路窃收、信息捕获、数据欺骗、异步攻击和伪造证件等。

目前全世界每年被计算机罪犯盗走的资金达200多亿美元,许多发达国家每年损失几十亿美元,计算机犯罪损失常常是常规犯罪的几十至几百倍。

计算机犯罪具有以下明显特征:采用先进技术、作案时间短、作案容易且不留痕迹、犯罪区域广、内部工作人员和青少年犯罪日趋严重等。

4. 计算机病毒

计算机病毒是利用计算机软件与硬件的缺陷或操作系统漏洞,由被感染机内部发出的破坏计算机数据并影响计算机正常工作的一组指令集或程序代码。它的产生和蔓延给计算机系统的可靠性和安全性带来严重威胁和巨大损失。

现今计算机病毒主要通过传统计算机病毒、蠕虫病毒、特洛伊木马、脚本病毒、手机病毒等几类进行攻击的。在现代化战争中可以利用传染病毒来破坏对方的军事指挥通信系统,使其处于瘫痪状态。

1.2.3 攻击与威胁计算机系统的来源

攻击与威胁计算机系统的来源可以分为自然因素和人为因素。

1. 自然因素

计算机系统所面临的威胁的自然因素是指计算机的使用环境等不具备安全条件，包括计算机硬件的失效、掉电、水灾与火灾等自然灾害的袭击，以及计算机使用环境不合乎要求等。

不同功能的硬件失效会带来不同的损失，例如，显示器失效，可以再买来一个换上，计算机照常运行，最危险的是硬盘失效，硬盘上的数据毁于一旦，如果你还没来得及备份，那么，你的心血也付之东流。所以，计算机数据信息的及时备份非常重要。

突然掉电可能会丢失储存在 RAM 中的数据，UPS(不间断电源供应设备)是一个含有电池以及其他电路的设备，能够持续供电，并在短暂的停电中为你的计算机继续供电，给你充足的时间来保存文件，停止程序的运行等，所以，应该有一个 UPS 来做应急帮助。

水灾、火灾等自然灾害是人类难以应付的，但是，如果经常备份数据，并为计算机加入保险，就会把损失降到最低点。

2. 人为因素

计算机系统面临的威胁的人为因素是指由于人的主观行为而造成的破坏，包括不经意的错误操作、故意的犯罪行为等。

不经意的错误操作最有可能导致数据的丢失和损坏，出比较常见的错误操作有：

(1) 在备份文档时，不小心用旧版本的文档覆盖了新版本的文档。

(2) 将包含重要数据的磁盘格式化。

(3) 数据输入错误。

故意的犯罪行为是指故意泄露或破坏计算机信息系统中的机密信息，以及危害系统实体安全、运行安全和信息安全的不法行为。

1.2.4 攻击与威胁计算机系统的人员

攻击与威胁计算机系统的人为因素中，根据造成攻击与威胁的人员对计算机的接近程度的不同，可以分为以下 4 类。

1. 外部人员

不能进入计算机中心或计算机房的人员。由于外部人员不能进入计算机中心，因此他们只能在外面进行攻击，主要攻击目标是网络中的通信线路等外部设施，可能造成的威胁有以下几种。

(1) 搭线窃听：在计算机的通信线路上搭上一个侦听设备，从而获得线路上传输的机密信息。

(2) 电磁辐射：通过接受计算机系统辐射出的信号而获得机密信息。

(3) 口令猜测：通过猜测口令而进入到网络系统中。

(4) 密文分析：通过分析线路上传输的加密信息而得到明文。

(5) 流量分析：通过观察通信线路上的信息流量，得到信息的源点和终点以及发送

频率等,从而推断出信息的某些重要特性。

(6) 愚弄:愚弄或欺骗计算机中心的人员,从而达到非法目的。

防止这类攻击的唯一有效办法是,将通信线路上的信息加密,并且在网络中实行可靠的协议,防止信息在加密之前从机房中泄露出去。

2. 物理存取人员

这类人员能进入计算机中心但没有多少上机的权利。他们的主要攻击目标是计算机中心内部,可能造成的威胁有如下几种。

(1) 窃听:将窃听器安装在中心里,录下中心人员之间的谈话。

(2) 窥视:站在终端用户身后,观察其操作过程。

(3) 插入:当用户离开终端后,攻击者利用仍开着的终端做他自己的事情。

(4) 蒙面:在计算机中心的某些地方,得到粗心大意的人写下的口令,从而冒称该人,使用计算机。

(5) 推导:从统计数据库中获得的统计信息出发,推导出某些不应该知道的信息。

(6) 浏览:通过观察中心内部的情况或计算机中的某些公用文件而获得有用的信息。

(7) 废物:从当作废物的打印纸中寻找有用的信息。

(8) 设备安装:攻击者将 EPROM(erasable programmable ROM,可擦除可编程ROM)或类似的电路芯片替换并重新插入计算机中,使计算机按照攻击者的目的运行。

对于这些攻击,有效的防范办法是:加强机房的出入管理,包括人员的进出管理和记录机密信息的媒介出入机房的管理。

3. 系统存取人员

这类人员通常是计算机中心的普通用户,他们在系统里拥有的权利不是太多。

他们能够实际操作计算机,具有较大的危险性,可能造成的威胁有如下几种。

(1) 强制崩溃:在程序中制造某些故意的错误,强制使计算机停止运转。

(2) 天窗:有些操作系统为了日后的维护而留下了入口,攻击者可利用这些入口作为进入操作系统的天窗。

(3) 聚合:将能合法得到的几项信息综合起来,从而知道一些不应该知道的保密信息。

(4) 复制:将有关程序和数据复制下来带出计算机中心。

(5) 骚扰:攻击者在终端上做出某些令操作人员生气的事情,使其容易发生错误,从而达到自己的目的。

他们具有的特权比较少,很想扩大自己的特权,系统管理员要严密监视他们的工作,特别注意一些奇异现象的发生,如计算机发生的崩溃次数太多等,要立即采取有效措施。

4. 编程特权人员

这类人员能在计算机上编制自己的程序,通常是指那些系统编程人员和系统维护人员。

他们通常是能够深入到系统中的人，构成的威胁极大，有以下几种。

(1) 特洛伊木马：修改某些程序，使得这些程序仍能正常工作，看上去是好的，实际上其中隐藏着一些破坏性的指令。

(2) 逻辑炸弹：一种只有当特定事件出现才进行破坏的程序。

(3) 病毒：实际上是一种逻辑炸弹，不同之处在于它不断地繁殖其自身。

(4) 滥用实用程序：有些计算机上的实用程序可以被修改以满足不同的需要，攻击者可利用实用程序达到自己的目的。

(5) 意大利香肠术：这是对财务系统进行的攻击。它从每个客户的账目中偷出一点点钱，客户往往不注意这种微弱损失，而攻击者将众多客户的钱加在一起，其数目巨大。

1.3 计算机安全保护的原则与措施

计算机系统安全技术涉及面广，本节主要介绍研究计算机安全问题的重要性、防护的基本原则和基本措施。

1.3.1 研究计算机安全问题的重要性

由于计算机系统本身存在的安全漏洞以及外在自然、人为因素的影响与破坏，计算机用户的利益随时都可能遭受损失，因此，研究计算机的安全问题至关重要，其重要性具体体现在以下几个方面。

(1) 计算机系统存储和处理的是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或是个人的敏感信息、隐私，因此必须安全保护这些信息不被敌对势力、不法分子攻击与威胁。

(2) 随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是随着 Internet 的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

(3) 人们对计算机系统的需求在不断扩大，这类需求在许多方面都是不可逆转、不可替代的，而计算机系统使用的场所正在转向工业、农业、野外、天空、海上、宇宙空间，核辐射环境等，这些环境都比机房恶劣，出错率和故障的增多必将导致可靠性和安全性的降低。

(4) 随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全功能不足。

(5) 计算机安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

(6) 从认识论的角度看，人们往往首先关注系统的功能，然后才被动地从现象注意系

统应用的安全问题，因此存在着重应用、轻安全、法律意识淡薄的普遍现象。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的。

1.3.2 安全保护的基本原则

计算机安全保护难度大，投资高，甚至远远超过计算机系统本身的价格。因此，实施计算机安全保护时应根据计算机系统的重要性，划分出不同的等级，实施相应的安全保护。需要统一的组织和指挥，不能装门面，搞排场。按照计算机安全的基本思想，可以参考如下计算机系统安全保护的基本原则。

1. 价值等价原则

价值等价不是价格等价，计算机系统硬软件费用的总和代表了价格，而它的价值与它处理的信息直接相关。例如，花 1 万元购进的一台普通微机，用于一般的文字处理服务，它的价值基本上与价格相等；若将这台微机用于国防或尖端科学技术信息管理，那么它的价值远远高于它的价格。计算机系统的价值与系统的安全等级有关，安全等级是根据价格与处理信息的重要性来综合评估的，是计算机系统实际价值的关键性权值。因此，在对计算机系统实施安全保护时，要看是否值得，对一般用途的少投入，对于涉及国家安全、社会安定等的重要系统要多投入。

2. 综合治理原则

计算机系统的安全保护是一个综合性的问题，一方面要采用各种技术手段来提高安全防御能力，如数据加密、口令机制、电磁屏蔽、防火墙技术及各种监视、报警系统等，另一方面要加强法制建设和宣传，对计算机犯罪行为进行严厉的打击。同时也要加强安全管理和安全教育，建立健全计算机系统的安全管理制度，通过多种形式的安全培训和教育，提高系统使用人员的安全技术水平，增强他们的安全意识。

3. 突出重点的原则

《中华人民共和国计算机信息系统安全保护条例》中第一章第四条明确规定：“计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。”

4. 同步原则

同步原则是指计算机系统安全保护在系统设计时应纳入总体进行考虑，避免在今后增加安全保护设施时造成应用系统和安全保护系统之间的冲突和矛盾，达不到应该达到的安全保护目标。同步的另一层含义是计算机系统在运行期间应按其安全保护等级实施相应的安全保护。

1.3.3 安全保护的基本措施

1. 安全立法

法律是规范人们一般社会行为的准则。它从形式上分有宪法、法律、法规、法令、条令、条例和实施办法、实施细则等多种形式。有关计算机系统的法律、法规和条例在内容上大体可以分成两类,即社会规范和技术规范。

(1) 社会规范是调整信息活动中人与人之间的行为准则。要结合专门的保护要求来定义合法的信息实践,并保护合法的信息实践活动,对于不正当的信息活动要受到民法和刑法的限制或惩处。它发布阻止任何违反规定要求的法令或禁令,明确系统人员和最终用户应该履行的权利和义务,包括宪法、保密法、数据保护法、计算机安全保护条例、计算机犯罪法等。

为了打击越来越多的通过计算机犯罪的行为,世界各国纷纷出台相应的法律、法规。但是,一般而言,受多方面因素的影响,保障计算机安全的法律体系尚欠完善,国家或地区之间也存在着较大的差异。近年来,我国公安部和国家保密局等机构为了加强对计算机信息网络国际联网的安全保护,维护公共秩序和社会稳定,制定了一系列的法律、法规,为计算机安全提供了可靠的保障。目前,我国在计算机安全方面的法律法规包括如下。

① 中国计算机信息网络国际联网管理暂行规定实施办法。

② 计算机信息系统国际联网保密暂行规定。

③ 计算机信息网络国际联网安全保护管理办法。

④ 计算机信息系统安全专用产品检测和许可证管理办法。

⑤ 计算机软件保护条例。

⑥ 商用密码管理条例。

⑦ 中华人民共和国保守国家秘密法。

⑧ 中华人民共和国计算机信息系统安全保护条例。

⑨ 中华人民共和国国家安全法。

(2) 技术规范是调整人和物、人和自然界之间的关系准则。其内容十分广泛,包括各种技术标准和规程,如计算机安全标准、网络安全标准、操作系统安全标准、数据和信息安全标准、电磁泄露安全极限标准等。这些法律和技术标准是保证计算机系统安全的依据和主要的社会保障。

2. 安全管理

安全管理主要是指一般的管理措施,即介于社会和技术措施之间的组织单位所属范围内的措施。从人事资源管理到资产物业管理,从教育培训、资格认证到人事考核鉴定制度,从动态运行机制到日常工作规范、岗位责任制度,方方面面的规章制度是一切技术措施得以贯彻实施的重要保证。所谓“三分技术,七分管理”的表现即在于此。

安全管理是计算机系统安全保护中的重要环节,这是国内外专家学者的共识,并在实践中得到了充分的证实。《中华人民共和国计算机信息系统安全保护条例》第十三条明确

规定："计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。"这说明计算机信息系统的安全保护责任落到了使用单位的肩上，各单位应根据本单位计算机信息系统的安全级别，做好组织建设和制度建设。

（1）组织建设。

计算机系统安全保护的组织建设是安全管理的根本保证，单位最高领导必须主管计算机信息系统的安全保护工作，成立专门的安全保护机构，根据本单位系统的安全级别设置多个专兼职岗位，做好工作的分工和责任落实，绝不能只由计算机信息系统的具体使用部门一家来独立管理。在安全管理机构的人员构成上应做到"三结合"，即领导、保卫人员和计算机技术人员相互结合。在技术人员方面还应考虑各个专业的适当搭配，如系统分析人员、硬件技术人员、软件技术人员、网络技术人员及通信技术人员等。安全管理机构应该定期组织人员对本单位计算机信息的安全情况进行检查，发现问题应及时解决；组织建立健全各项安全管理制度，并经常监督其执行情况；对各种安全设施设备定期检查其有效性，保证其功能的正常发挥。除此以外，还应对当前易遭到的攻击进行分析和预测，并采取适当措施加以防备。

（2）制度建设。

只有搞好制度建设，才能将计算机系统的安全管理落到实处，做到各种行为有章可循，职责分明。安全管理制度应该包含以下几个方面的内容。

① 保密制度：对于有保密要求的计算机信息系统，必须建立此项制度。首先应对各种资料和数据按有关规定划分为绝密、机密、秘密三个保密等级，制定出相应的访问、查询及修改的限制条款，并对用户设置相应的权限。对于违反保密制度规定的应对其做出相应处罚，直至追究刑事责任，移送公安机关。

② 人事管理制度：对计算机系统的管理和使用人员调出和调入做出一些管理规定。主要有政治审查、技术审查及上网安全培训、调离条件及保密责任等内容。

③ 环境安全制度：环境安全制度应包括机房建筑环境、防火防盗防水、消防设备、供电线路、危险物品以及室内温度等建立相应的管理规定。

④ 出入管理制度：包括登记制度、验证制度、着装制度以及钥匙管理制度等。

⑤ 操作与维护制度：操作规程的制定是计算机信息系统正确使用的纲领，在制定时应科学化、规范化。系统的维护是正常运行的保证，通过维护及早发现问题，避免很多安全事故的发生。在制定维护制度时，应对重点维护、全面维护、维护方法等做出具体规定。

⑥ 日志管理及交接班制度：日志是计算机信息系统一天的详细运行情况的记载，分为人工记录日志和计算机自动记录日志两部分。制定该制度时，在保证日志的完整性、准确性及可用性等方面做出详细的规定。交接班制度是落实责任的一种管理方式，应对交接班的时间、交接班时应交接的内容做出规定，交接班人应在记录上签名。

⑦ 器材管理制度：器材，尤其是应急器材是解决安全事故的物质保证，应对器材存储的位置、环境条件、数量多少、进货渠道等方面做出详细的规定。

⑧ 计算机病毒防治制度：计算机病毒已经成为了影响计算机信息系统安全的大敌。该制度中应该对防止病毒的硬、软件做出具体规定，对于防毒软件一般要求两种以上，并应定期进行病毒检查和清除。对病毒的来源应严格加以封锁，不允许外来磁盘上机，不运

行来源不明的软件，更不允许编制病毒程序。

以上仅列举了部分管理制度，对于具体的计算机系统，可以根据具体情况进行增删。

3. 技术措施

计算机安全技术措施是计算机系统安全的重要保证，也是整个计算机系统安全的物质技术基础。实施计算机安全技术，不仅涉及计算机和外部设备，还涉及数据安全、软件安全、网络安全、数据库安全、运行安全、防病毒技术、站点安全以及系统结构、工艺和保密、压缩技术。安全技术措施的实施应贯彻落实在系统开发的各个阶段，从系统规划、系统分析、系统设计、系统实施、系统评价到系统的运行、维护和管理。

1.4 计算机安全技术

计算机安全技术是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，它的主要任务是研究计算机系统和通信网络内信息的保护方法以实现系统内信息的安全、保密、真实和完整。

计算机安全技术是对实体安全、运行安全、信息安全和网络安全实施保护所采用的技术手段，是一种主动保护措施，用来提供计算机系统安全、增强计算机系统防御攻击和破坏的能力。

本节主要介绍计算机安全技术的内容与发展趋势。

1.4.1 计算机安全技术简介

针对计算机安全目标以及安全性问题，本书所指的计算机安全技术主要由实体安全技术、软件安全技术、密码技术、操作系统安全技术、数据库系统安全技术、病毒防治技术、网络攻防技术、应用安全技术、应急响应与灾难恢复技术等组成。

1. 实体安全技术

实体安全在整个计算机网络信息系统安全体系中占有重要地位。计算机信息系统安全的内涵是保护计算机信息系统硬件设备、基础设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。它包含的主要内容为环境安全、设备安全、电源系统安全和通信线路安全。

（1）环境安全。

计算机网络通信系统的运行环境应按照国家有关标准设计实施，应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗系统报警，以保护系统免受水、火、有害气体、地震、静电等的危害。

（2）设备安全。

要保证设备随时处于良好的工作状态，应当建立、健全使用管理规章制度，建立设备运行日志。同时要注意保护存储介质的安全性，包括存储介质自身和数据的安全。存储介质本身的安全主要指安全保管、防盗、防毁和防霉；数据安全是指防止数据被非法复制和销毁。

(3) 电源系统安全。

电源是所有电子设备正常工作的能量源,在信息系统中占有重要地位。电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

(4) 通信线路安全。

通信设备和通信线路的装置安装要稳固牢靠,具有一定对抗自然因素和人为因素破坏的能力。它包括防止电磁信息的泄露、线路截获以及抗电磁干扰。

2. 密码技术

密码技术是保障信息安全的核心技术,是对信息进行加密与解密的技术,加解密技术的核心又是加密算法与解密算法。密码技术是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科,它不仅具有保证信息机密性的加密功能,而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以,使用密码技术不仅可以保证信息的机密性,而且可以保证信息的完整性和确定性,防止信息被篡改、伪造和假冒。

3. 软件安全技术

软件安全的主要目的:一是禁止非法复制和使用,二是防止非法阅读和修改。

根据不同的软件保护目的,存在不同的软件安全技术。从防止软件非法复制的角度考虑,有软件防复制技术和软件加密技术。软件防复制技术的主要方法包括硬件防复制,软件防复制,软硬件结合。软件加密技术大致可分为软加密与硬加密。从保障软件质量、防止软件被破解的角度考虑,有软件分析技术。

4. 操作系统安全技术

操作系统的安全技术主要包括标识与鉴别、自主访问控制(discretionary access control,DAC)、强制访问控制(mandatory access control,MAC)、安全审计、客体重用、最小特权管理、可信路径、隐蔽通道分析、加密卡支持等。

5. 数据库系统安全技术

数据库安全性问题一直是数据库用户非常关心的问题。数据库往往保存着生产和工作需要的重要数据和资料,数据库数据的丢失以及数据库被非法用户的侵入往往会造成无法估量的损失,因此,数据库的安全保密成为网络安全防护中需要非常重视的环节,要维护数据信息的完整性、保密性、可用性。

6. 网络攻防技术

网络安全已成为人们在信息空间中生存与发展的重要保证条件,与国家的政治安全、经济安全、军事安全、社会稳定以及人们的日常生活关系密切 。由于一些人受兴趣爱好和经济利益的驱使,网络攻击事件层出不穷。公司和国家只有积极防御,才能在攻击环境下生存。

攻击与防御是一对既相互制约又相互发展的网络安全技术。面对黑客不断开发的新

的攻击技术，防御技术也必须不断更新。但是应当看到，正是攻击技术的不断发展才使得防御技术日新月异。同时，这两种技术也是互相转化的，不同的人抱着不同的目的来使用同一种技术，这种技术既可以攻击又可以防御攻击，例如网络监听技术，黑客可以使用网络监听技术去监听目标网络传输的信息，同时也可以采用这种技术监听自己的网络是否发生异常。

网络防御技术包括加密、操作系统安全配置（网络节点）、防火墙、入侵检测等。

7. 应用安全技术

目前，全球互联网用户已达 15 亿，网络已经成为人们生活中的一部分，大部分用户利用 Web 站点对网页进行访问，并利用网络进行购物及通过网上银行进行网上支付；同时，部分用户和企业使用电子邮件、FTP 等进行文件传输，利用 QQ 聊天等方式进行网上办公。但人们在享受便捷网络的同时，网络应用的安全威胁也日益严重，例如 IP 地址欺骗、网络钓鱼、网页病毒、QQ 被盗、垃圾邮件等。因此，对于每一个使用网络的人来说，掌握一些应用安全措施及技术是很有必要的。其中应用安全措施主要包括口令、E-mail、QQ 使用、网上购物与网上支付等在使用过程中的安全措施，应用安全技术则主要包括网络防钓鱼技术，网络防肉鸡技术，网络监听技术，扫描器技术等。

8. 应急响应与灾难恢复技术

应急响应是指一个组织为了应对各种安全事件的发生所做的准备工作以及在突发事件发生时或者发生后所采取的措施。

灾难恢复是将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设计的活动和流程。

1.4.2 计算机安全技术的发展

1. 计算机安全技术的发展阶段

美国国防部（DoD）为抵御越来越严重的面向国防信息的攻击和侵入（黑客、病毒等）威胁，国防高级研究计划局（DARPA）启动了一个大型的研究计划——“第三代安全技术”（third generation security，3GS），项目的具体名称叫做“有机保障和存活的信息系统”（organically assured and survivable information systems，OASIS ）。包含 30 多个研究容侵关键技术（容忍攻击和侵入）的子课题。OASIS 的技术报告（2003）中，将计算机安全技术划分为 4 个阶段。

（1）第一阶段：加密系统。

第一代计算机安全技术的设计理念是借助于密码技术、可信计算基（trusted computing base，TCB）、认证技术和访问控制技术等，来遏止恶意入侵的发生。

（2）第二阶段：防御系统。

第二代计算机安全技术的设计，融入了防火墙、入侵检测技术，预将入侵者“御之国门之外”。

前两个阶段的技术是希望建造“金刚不坏，百毒不侵”的信息系统，但无论花费多大的代价，完美系统是构造不出来的。对来自“内部”的攻击，缺乏防御能力，对新的（未知）攻击的方法和方式，缺乏防御能力，所以外部攻击或侵入也时常成功，恶意事件时常发生，即使运用了所有的可行技术，一些攻击还是无法避免。所以，重要的信息系统必须能够容忍系统故障或入侵的发生，并且能够继续工作。这就是第三阶段的计算机安全技术——容侵。

（3）第三阶段：容侵系统。

容侵把系统受到入侵和攻击后的不正确行为，也当作一种系统故障，利用容错技术，来保证系统的正确执行。这实质上，是着重于运行结果，而不纠缠于错误原因。OASIS所倡导的容侵技术可能需要一段时间才能够广泛融入到现有的系统中，DARPA 将继续扶植这一领域的研究。

（4）第四阶段：自恢复系统（self-regenerative systems）。

自恢复的信息系统能够在受到攻击的情况下，自动重新组织，自我恢复。这样的系统必须具有自我诊断，自我修复，主动感知和适应外部运行环境（自动重新配置运行参数）等功能，并将自治性、智能学习等功能嵌入到“容侵”系统中，使其能抵御未知的攻击类型。

第三代和未来第四代的安全技术的理念是使系统“带病工作、自我恢复”。

欧洲的 MAFTIA 项目也启动了对恶意攻击和故障的容忍技术研究。

2. 计算机安全技术发展的特点

计算机安全技术的发展主要呈现 4 个特点。

（1）可信化。

这个特点是指从传统计算机安全理念过渡到以可信计算理念为核心的计算机安全。近年来，计算机安全问题愈演愈烈，传统安全理念很难有所突破，人们试图利用可信计算的理念来解决计算机安全问题，其主要思想是在硬件平台上引入安全芯片，从而将部分或整个计算平台变为“可信”的计算平台。目前还有很多问题需要研究和探索，如基于 TCP 的访问控制、基于 TCP 的安全操作系统、基于 TCP 的安全中间件、基于 TCP 的安全应用等。

（2）网络化。

由网络应用和普及引发的技术和应用模式的变革，正在进一步推动信息安全关键技术的创新发展，并诱发新技术和应用模式的出现。如安全中间件，安全管理与安全监控都是网络化发展带来的必然的发展方向；网络病毒和垃圾信息防范都是网络化带来的一些安全性问题，网络可生存性、网络信任都是要继续研究的领域。

（3）标准化。

发达国家和地区高度重视标准化的趋势，现在正逐步渗透到发展中国家。安全技术要走向国际，走向应用，我国政府、产业界、学术界正高度重视信息安全标准的研究与制订工作，如密码算法类标准（加密算法、签名算法、密码算法接口）、安全认证与授权类标准（PKI、PMI、生物认证）、安全评估类标准（安全评估准则、方法、规范）、系统与网络类安全

标准(安全体系结构、安全操作系统、安全数据库、安全路由器、可信计算平台)、安全管理类标准(防信息遗漏、质量保证、机房设计)等。

(4) 集成化。

即从单一功能的信息安全技术与产品,向多种功能融于某一个产品,或者是几个功能相结合的集成化的产品转化,产品不再以单一的形式出现,否则产品太多,不利于推广和应用。安全产品呈硬件化和芯片化发展趋势,将带来更高的安全度与更高的运算速度。也需要发展更灵活的安全芯片的实现技术,特别是密码芯片的物理防护机制。

1.5 计算机安全评估

计算机安全评估是对计算机一个构件、产品、子系统或系统的安全属性进行的技术评价,通过评估判断该构件、产品、子系统或系统是否满足一组特定的要求。

本节主要介绍计算机安全评估的意义与安全标准。

1.5.1 计算机安全评估的意义

计算机安全评估的意义在于了解计算机的安全现状,了解计算机的安全需求,为建立计算机系统安全管理制度,制定安全策略和实施安防措施提供依据,为组织实现计算机安全提供评估标准。

安全评估服务是指依据国家有关信息安全技术的标准,对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价的过程,它主要评估信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响,估计每种攻击的代价,估算出可能的应对措施的费用,选择恰当的安全机制。

1.5.2 计算机系统安全标准

20 世纪 70 年代,美国国防部就已经发布了诸如“自动数据处理系统安全要求”等一系列的安全评估标准。1983 年又发布了“可信计算机评价标准”,即所谓的橙皮书、黄皮书、红皮书和绿皮书,并于 1985 年对此标准进行了修订。

我国从 20 世纪 80 年代开始,本着积极采用国际标准的原则,转化了一批国际信息安全基础技术标准,有关的信息安全标准有《计算机信息系统安全专用产品分类原则》、《计算机信息系统安全保护等级划分准则》、《商用密码管理条例》、《中华人民共和国计算机信息系统安全保护条例》等。

下面介绍计算机安全评估目前常见的标准。

1. OSI 安全体系结构的 5 种安全服务项目

国际标准化组织在 ISO 7498—2 中描述的开放系统互连 OSI 安全体系结构的 5 种安全服务项目如下所示。

(1) 鉴别服务(authentication):提供对通信中的对等实体和数据来源的鉴别。对等实体鉴别是指确认有关的对等实体是所需的实体;数据原发鉴别是指确认接收到的数据

的来源是所要求的。

(2) 访问控制服务(access control):防止对资源的非授权使用,包括防止以未授权方式使用某一资源。

(3) 数据机密性服务(data confidentiality):对数据提供保护,使之不被非授权地泄露。包括连接机密性、无连接机密性、选择字段机密性以及通信业务流机密性。

(4) 数据完整性服务(data integrity):用来对付主动威胁,包括带恢复的连接完整性、无恢复的连接完整性、选择字段的连接完整性、无连接完整性以及选择字段无连接完整性。

(5) 抗否认服务(non-reputation):包括两种形式,有数据原发证明的抗否认与有交付证明的抗否认。

2. OSI 安全体系结构的 8 种安全机制

为了实现以上 5 种安全服务,ISO 制定了 8 种安全机制。

(1) 加密机制(encipherement mechanisms)。

加密既能为数据提供机密性,也能为通信业务流信息提供机密性,并且是其他安全机制中的一部分或对安全机制起补充作用。加密算法可以是可逆的,也可以是不可逆的。除了某些不可逆加密算法的情况外,加密机制的存在意味着要使用密钥管理机制。

(2) 数字签名机制(digital signature mechanisms)。

签名过程使用签名者的私有信息作为私钥,或对数据单元进行加密,或产生出该数据单元的一个密码校验值,验证过程使用公开的规程与信息来决定该签名是否是用签名者的私有信息产生的,签名过程的本质特征为该签名只有使用签名者的私有信息才能产生出来。

(3) 访问控制机制(access control mechanisms)。

访问控制机制包括访问控制信息库、鉴别信息、权利与安全标记。

(4) 数据完整性机制(data integrity mechanisms)。

数据完整性机制包括:单个数据单元或字段的完整性,数据单元流或字段流的完整性。

(5) 鉴别交换机制(authentication mechanisms)。

鉴别交换机制包括:使用鉴别信息(如口令),由发送实体提供而由接收实体验证;密码技术;使用该实体的特征或占有物。

(6) 通信业务填充机制(traffic padding mechanisms)。

通信业务填充机制用来提供各种不同级别的保护,对抗通信业务分析,只有在通信业务填充受到机制服务保护时才是有效的。

(7) 路由选择控制机制(routing control mechanisms)。

路由选择控制机制包括:路由能动态地或预定地选取,以便只使用物理上安全的子网络、中继站或链路;在检测到持续的操作攻击时,端系统可以指示网络服务的提供者经不同的路由建立连接;带有某些安全标记的数据可能被安全策略禁止通过某些子网络、中继站或链路。

(8) 公证机制(notarization mechanisms)。

有关在两个或多个实体之间通信的数据的性质,能够借助公证机制得到确保,这种保证是由第三方公证人提供的,公证人为通信实体所信任,并掌握必要信息以一种可证实方式提供所需的保证。

5 种安全服务和 8 种安全机制的关系见表 1-1。

表 1-1　安全服务与安全机制的关系

安全机制 / 安全服务	加密机制	数字签名机制	访问控制机制	数据完整性机制	鉴别交换机制	通信业务填充机制	路由控制机制	公正机制
对等实体鉴别	Y	Y		Y				
数据源鉴别	Y	Y						
访问控制			Y					
连接有保密	Y						Y	
连接无保密	Y						Y	
信息流保密						Y		
可否恢复连接完整性	Y			Y				
选字段连接完整	Y		Y					
选字段无连接完整	Y	Y		Y				
无连接完整性	Y	Y		Y				
选择字段保密	Y							
抗来源否认		Y		Y				
抗交付否认		Y		Y				Y

注:Y 表示安全服务需要具有安全机制。

3. 美国国家计算机安全中心(NCSC)的可信系统评价准则

NCSC 领导着计算机和网络的研究工作,其提出的《可信计算机系统评测标准》(trusted computer system evaluation criteria,TCSEC),依据美国国防部发表的评估计算机系统安全等级的橙皮书,将计算机安全等级划分为 A、B、C、D 四类与 A1、B3、B2、B1、C2、C1、D 七级。不同计算机信息系统可以根据需要和可能选用不同安全保密强度的标准,如军事、国防为 A、B 类,金融、财贸为 B1、C2 级或更高级的计算机系统。可信系统评价准则见表 1-2。

4. 中国计算机信息系统安全保护等级划分准则

依据我国颁布的《计算机信息系统安全保护等级划分准则》(GB 17859—1999),计算机系统中全部保护机制的组合定义为可信计算机(TCB)。该标准将计算机安全等级划分为五级。

本标准规定了计算机系统安全保护能力的五个等级。

表 1-2　可信系统评价准则等级

类别	处理级别	名　　称	主要特征及适用范围
A	A1	验证设计	形式化最高级描述、验证和隐秘通道分析，非形式化代码对应证明，用于绝密级。
B	B3	安全域保护	存取监督器安全内核高抗渗透能力，可信恢复用于绝密、机密，即使系统崩溃，也不会泄密
	B2	结构化保护	隐秘通道约束，安全体系结构，较好的抗渗透能力，用于各级安全保密，实行强制性控制
	B1	标志的安全保护	强制存取控制，安全标记数据，对数据流监视
C	C2	受控制存取保护	独立的可查性，广泛的审核、跟踪，用于金融
	C1	自主安全保护	自主存取控制，多用户工作中防止事故的保护，也称无条件保护，早期 UNIX 系统属于此类
D	D	低级保护	不分等级，早期商业系统属于此类

第一级：用户自主保护级（相当于 C1 级）。本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力，对用户实施访问控制，即为用户提供可行的手段，保护用户和用户组信息，避免其他用户对数据的非法读写与破坏。

第二级：系统审计保护级（相当于 C2 级）。与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

第三级：安全标记保护级（相当于 B1 级，属强制保护）。本级的计算机信息系统可信计算基具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。

第四级：结构化保护级（相当于 B2 级）。本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。

第五级：访问验证保护级（相当于 B3-A1 级）。本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

本标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全

保护能力随着安全保护等级的增高而逐渐增强。

5. 其他重要技术标准

如安全电子交易协议(secure electronic transaction protocol,SET),美国国家标准化委员会 ANSI 的 DEI 及 RSA 加密算法标准等。

1.6 案例讨论

案例 1-1 计算机犯罪

世界上第一例受到法律追究的计算机犯罪事件发生在美国。1960 年美国斯坦福研究所发现一位计算机工程师通过修改程序的方法,篡改银行账目上的余额,为此,这位工程师受到了法办。20 世纪 70 年代以后,计算机犯罪开始大幅度增长。在过去的 20 多年中仅美国斯坦福研究所就记录了 3000 多起发生在世界各地的计算机犯罪案件,它们包括伪造、盗窃、间谍、共谋、勒索及计算机软硬件偷窃。

近年来,在西方一些发达国家,计算机犯罪每年都在疯狂增长,成为十分严重的社会问题。据报道美国计算机犯罪造成的损失已在千亿美元以上,年损失达几十亿至上百亿美元。英国、德国在这方面的年损失也达几十亿美元。为了对付计算机犯罪,美国在网络保安工作上花费了大量的财力,美国联邦调查局和一个著名智囊机构检查约 400 家公司和机构时,40%的公司和机构报告说最近遭受过侵入,其中约有 30%的入侵事件是突破防火墙从互联网络入侵的。英国的公司每年也要花 5.3 亿英镑来对付计算机伪造和入侵。英国计算机中心报告说,80%以上的英国公司在最近几年中安全系统受到破坏。

在我国关于计算机犯罪的报道也屡见不鲜,例如,大连市某银行办事处 ASC 6800 型计算机的一名管理员,利用由他通过计算机控制的“银行收贷款利息”的专用科目和“到期未归贷款利息”科目,把客户交来的贷款利息 11 万元截留,通过计算机转到同伙的账户上,汇出套取现金,受到法律的制裁。据不完全统计,我国在 1986 年到 1987 年查获过 9 起利用计算机进行犯罪的事件,1989 年查获上百起,1993 年达到 1200 多起。其数量呈直线上升。

通过案例,可以看出计算机安全关系到我们生活的方方面面。你认为,作为一个计算机使用者,应如何提高保护计算机安全的警惕性呢?

案例 1-2 网络战

早在 1991 年的海湾战争中,美军就对伊拉克实施了网络战。开战前,美国中央情报局派特工到伊拉克,将其从法国购买的防空系统使用的打印机芯片换上了含有计算机病毒的芯片。在战略空袭前,又用遥控手段激活了病毒,致使伊防空指挥中心主计算机系统程序错乱,防空 C3I 系统失灵。在 1999 年的科索沃战争中,网络战的规模和效果都有增无减。南联盟使用多种计算机病毒,组织“黑客”实施网络攻击,使北约军队的一些网站被垃圾信息阻塞,北约的一些计算机网络系统曾一度瘫痪。北约一方面强化网络防护措施,

另一方面实施网络反击战，将大量病毒和欺骗性信息注入南军计算机网络系统，致使南军防空系统陷于瘫痪。

2009 年 1 月，法国海军内部计算机系统的一台计算机受病毒入侵，迅速扩散到整个网络，一度不能启动，海军全部战斗机也因无法"下载飞行指令"而停飞两天。仅仅是法国海军内部计算机系统的时钟停摆，法国的国家安全就出现了一个偌大的"黑洞"。设想，如果是一个国家某一系统或领域的计算机网络系统出现问题或瘫痪，这种损失和危害将是不可想象的。

通过此案例，可以看出计算机安全关系到国家安全，你认为，国家应该采取哪些计算机安全措施呢？

归纳总结

1. 根据本章内容，归纳计算机存在哪些安全威胁。
2. 根据本章内容，归纳总结你认为需要哪些计算机安全技术。
3. 根据本章内容，讨论应该如何学习计算机安全技术。

思考与实践

思考题

1. 什么是计算机安全？如何评估计算机的安全状态？
2. 为什么要保证计算机的安全？
3. 计算机操作系统的脆弱性有哪些？
4. 进行计算机安全保护的原则和措施有哪些？
5. 保证计算机运行安全的技术有哪些？
6. 你是如何理解计算机安全技术结构的？

实践题

1. 上网了解目前计算机安全技术的发展趋势。
2. 上网搜集计算机安全问题的相关案例。
3. 用表格归纳总结你在使用计算机、U 盘以及上网中发现的计算机安全问题。



第2章 实体安全技术

学习目标

通过本章的学习，能够——

- 了解计算机硬件和基础设施安全的概念；
- 了解基础设施与环境安全；
- 知道计算机硬件和基础设施面临的威胁；
- 知道计算机硬件安全技术；
- 掌握计算机硬件常见故障的维护。

引导案例

2009年3月10日晚，广州市电子政务穗园电子政务计算机机房（以下简称机房）UPS电池发生击穿事故，冒起浓烟。经过约两个小时的扑救，现场浓烟得到有效控制，没有造成人员伤亡。事故导致该市政府门户网站、邮件系统、互联网出口、政务服务中心、住房公积金中心等重要系统一度无法使用。

后来经查明，这起事故原因认定为供电不稳定，导致恢复供电后产生的瞬时高压造成UPS电池短路，引发火灾。但是在火灾发生初期，计算机机房的防火设施并没有发挥作用，导致数台服务器和其他计算机相关设备不同程度的损坏，导致大量数据无法恢复，造成重大损失。

2.1 硬件和基础设施安全概述

本书中实体主要指计算机硬件和计算机基础设施。本节主要介绍硬件和基础设施的定义，并在此基础上介绍硬件和基础设施所面临的安全威胁，以及相应的安全防护方法。

2.1.1 硬件和基础设施的定义

1. 硬件的定义

硬件是指计算机系统中的电子元器件、各种线路及设备，硬件为计算机处理数据提供

物质基础。从功能上讲，计算机硬件系统主要由输入设备、输出设备、存储设备、运算器和控制器五部分组成（其中，运算器和控制器的集成芯片叫做中央处理器，即 CPU）。

计算机硬件的基本功能是接收计算机程序的控制来实现数据输入、运算、数据输出等一系列根本性的操作。虽然计算机的制造技术从计算机出现到今天已经发生了极大的变化，但在基本的硬件结构方面，一直沿袭着冯・诺依曼的传统框架，即计算机硬件系统由控制器、运算器、存储器、输入设备、输出设备五大基本部件构成。原始数据的程序通过输入设备送入存储器，在运算处理过程中，数据从存储器读入运算器进行运算，运算的结果存入存储器，必要时再经输出设备输出。指令也以数据形式存于存储器中，运算时指令由存储器送入控制器，由控制器控制各部件的工作。具体结构如图 2-1 所示。

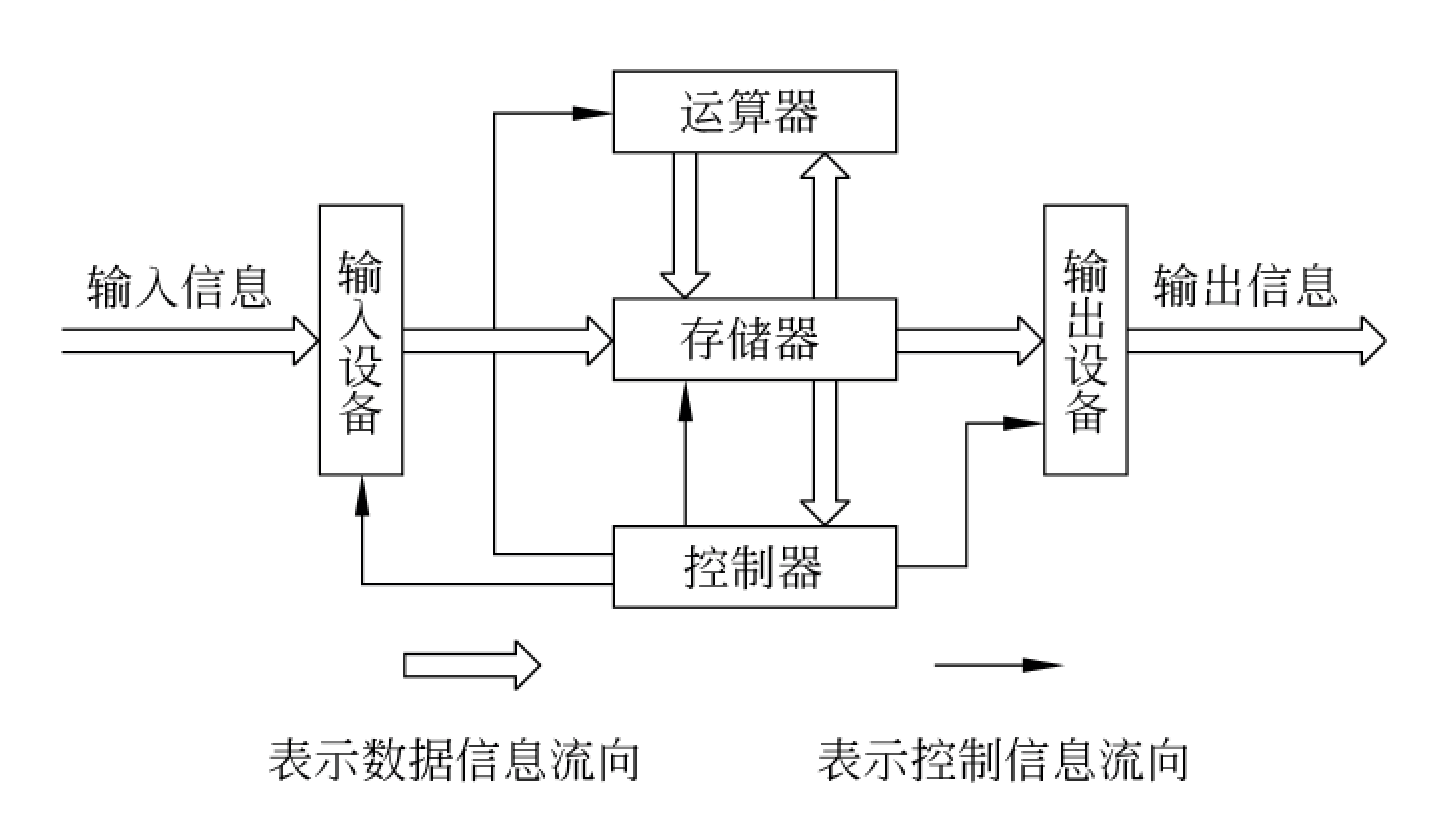


图 2-1　计算机基本结构

从计算机基本结构出发，计算机包括 CPU、存储器、输入设备、输出设备。

(1) CPU。

运算器和控制器是计算机的核心部件，大规模集成电路技术出现之后，这两个部件被集成到一块芯片上，称之为中央处理器（central processing unit，CPU）。CPU（如图 2-2 所示）是整个系统的核心，也是整个系统最高的执行单位，是决定计算机性能的核心部件。它负责整个系统指令的执行、数学与逻辑的运算、数据的存储与传送以及对内外输入输出的控制。

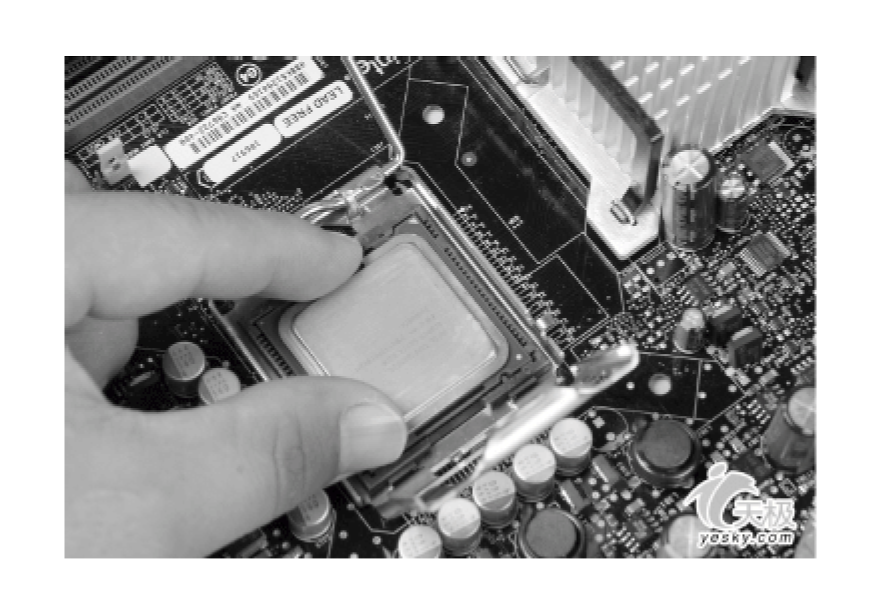




图 2-2　CPU 与风扇

从图 2-2 中可以看出，CPU 安装在 CPU 插座之上，然后，在 CPU 上面安装一个电风扇，用于散去 CPU 的热量。

(2) 存储器。

存储器是用来存储程序和数据的。CPU 可以直接访问的存储器称之为内存储器（又

称主存储器、内存),CPU 不能直接访问的存储器称之为外存储器(又称为辅助存储器)。

计算机所操作的数据是存储在内存之中的,内存是一个独立的部件,并以插卡式设计的,通常称之为内存条,如图 2-3 所示。

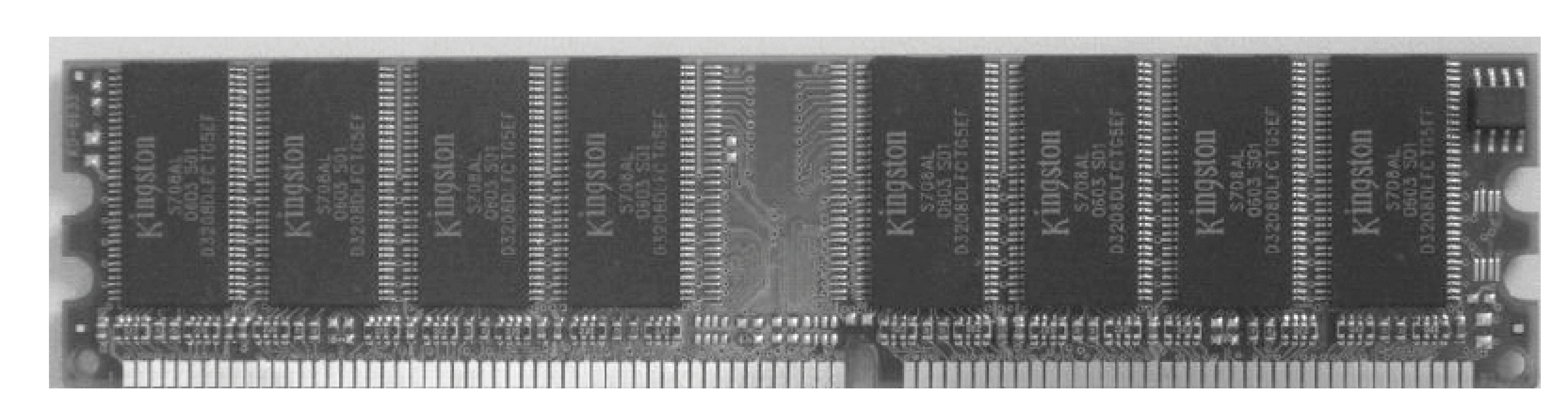


图 2-3 内存条

外储存器主要有硬盘、软盘、光盘、U 盘等,软盘存储器已经逐步被淘汰,现在一般个人计算机(PC)和笔记本计算机使用最多的是硬盘,硬盘驱动器如图 2-4 所示。

光盘存储器由于机械读写速度的原因,没有像硬盘存储那样灵活且速度快,所以,光存储器一般用于离线存储,也就是备份数据时使用。光盘存储器分为光盘驱动器、光盘塔和光盘库,最常用的光盘驱动器如图 2-5 所示。



图 2-4 硬盘驱动器



图 2-5 光盘驱动器

(3) 输入设备。

输入设备是计算机输入信息的装置,用于向计算机输入原始数据和处理这些数据的程序。常用的输入设备有键盘、鼠标、数字化仪、磁盘驱动器、模数转换器(A/D)等。

键盘是最常用也是最主要的输入设备,通过键盘,可以将英文字母、数字、标点符号等输入到计算机中,从而向计算机发出命令、输入数据等。台式计算机和笔记本计算机的键盘如图 2-6 所示。





图 2-6 计算机键盘

鼠标用来控制显示器所显示的指针光标。它从出现到现在已经有 40 年的历史了。鼠标的使用是为了使计算机的操作更加简便,用来代替键盘那些烦琐的指令。台式机和笔记本计算机的鼠标如图 2-7 所示。





图 2-7　鼠标

除此之外的输入设备,还有游戏杆、光笔、数码相机、数字摄像机、图像扫描仪、传真机、条形码阅读器、语音输入设备等。

(4) 输出设备。

输出设备主要用于将计算机处理过的信息传递出去,以人们能接受的数字、文字、符号、图形和图像等形式显示或者打印出来。常用的输出设备有显示器、打印机、磁盘驱动器、测绘仪、数字转换器(D/A)。

显示器的价格取决于所采用的显像管,好的显像管可以提供更好的视觉效果,寿命也更长,目前比较常见的显示器有 CRT 显示器和液晶显示器,如图 2-8 所示。




图 2-8　显示器

(5) 网络设备及部件。

除了 CPU、存储器、输入设备、输出设备以外,网络连接部件也是计算机硬件系统的组成部分。网络连接部件是连接到网络中的物理实体,其种类繁多,且与日俱增。基本的网络联接部件有集线器、网桥、网关、网络接口卡(NIC)、无线接入点(WAP)和调制解调器等。

2. 基础设施的定义

计算机基础设施是指为计算机用户提供公共服务的物理工程设施,是用于保证区域或者个人正常网络应用的服务系统。它是整个互联网赖以生存和发展的基础设施。

计算机基础设施不仅包括防火墙、路由器、交换机、远程访问设备(如 VPN 和拨号 Modem 池)等网络设备,而且包括机房建筑、机房环境、供电系统、空调等实体。

计算机基础设施为计算机的应用和信息共享提供平台,是整个计算机网络的重要支撑。在现代互联网发展中,计算机基础设施安全扮演着越来越重要的角色。

2.1.2　硬件和基础设施的安全威胁

1. 硬件自身的安全威胁

(1) 硬件丢失。

PC 的一个重要用途是建立个人办公环境,可以放在办公室的办公桌上。这样虽然

方便办公，但安全隐患很大。与大型计算机相比，大多数 PC 无硬件级的保护，他人很容易操纵控制计算机。即使有保护机制也很简单，很容易被绕过。例如，保存计算机基本启动信息（日期、时间、启动设置等）的芯片 CMOS（complementary metal oxide semiconductor）中的口令机制可以通过把 CMOS 的供电电池短路，使 CMOS 电路失去记忆功能，而绕过口令的控制。由于 PC 的机箱很容易打开（有的计算机甚至连螺丝刀也不需要），做到这一点是很容易的。

计算机硬件的尺寸越来越小，容易搬移，尤其是便携机更是如此。这既是优点，也是弱点。这样小的计算机并未设计固定装置，计算机能方便地安放在桌面上，盗窃者很容易搬走整个计算机，其中的各种文件更谈不上安全问题了。

计算机的外部设备不受操作系统安全控制，任何人都可以利用系统提供的输出命令打印文件内容，输出设备最容易造成信息泄露或整个被窃取。

PC 的硬盘很容易安装，也容易拆卸和被偷盗，存储在硬盘上的文件几乎没有任何保护措施，DOS 文件系统的存储结构与管理方法几乎是人所皆知的，文件的安全属性，如隐藏、只读、独占等属性，很容易被修改，对磁盘文件目录区的修改既没有软件保护，也没有硬件保护，掌握磁盘管理工具的人，很容易更改磁盘文件目录区，造成整个系统的信息紊乱。

（2）信息泄露。

在硬盘或软盘的磁介质表面的残留磁信息是重要的信息泄露渠道，文件删除操作仅仅在文件目录中做了标记，并没有删除文件本身数据存储区，有经验的用户可以很容易地恢复被删除的文件。保存在软盘上的数据很容易因不小心划坏、各种硬碰伤或受潮霉变而无法利用。

内存空间之间没有保护机制，即使简单的界限寄存器也没有，也没有只可供操作系统使用的监控程序或特权指令，任何人都可以编制程序访问内存的任何区域，甚至连系统工作区（如系统的中断向量区）也可以修改，用户的数据区得不到硬件提供的安全保障。

计算机中的显示器、中央处理器（CPU）和总线等部件在运行过程中能够向外部辐射电磁波，电磁波反映了计算机内部信息的变化。经实际仪器测试，在几百米以外的距离可以接受与复现显示器上显示的信息，计算机屏幕上的信息可以在其所有者毫不知晓的情况下泄露出去。计算机电磁泄漏是一种很严重的信息泄露途径。

计算机硬件故障也会对计算机中的信息造成威胁，硬件故障常常会使正常的信息流中断，在实时控制系统中，这将造成历史信息的永久丢失；磁盘存储器磁介质的磨损或机械故障使磁盘文件遭到损坏。这些情况都会破坏信息的完整性。

2. 基础设施的安全威胁

基础设施的主要安全威胁有：

（1）计算机及其基础设施自身存在的脆弱性因素；

（2）各种自然灾害等环境因素导致的安全问题；

（3）由于人为的错误操作及各种计算机犯罪导致的安全问题。

3. 环境对硬件和基础设施的安全威胁

(1) 温度。

计算机的电子元器件、芯片都密封在机箱中，有的芯片工作时表面温度相当高，例如586CPU芯片需要带一个小风扇散热，电源部件也是一个大的热源，虽然机箱后面有小型排风扇，但计算机工作时，箱内的温度仍然相当高，如果周边温度也比较高的话，机箱内的温度很难降下来。

一般电子元器件工作温度的范围是0℃～45℃，当环境温度超过60℃时，计算机系统就不能正常工作，温度每升高10℃，电子元器件的可靠性就会降低25%。元器件可靠性降低无疑将影响计算机的正确运算，影响结果的正确性。

(2) 湿度。

环境的相对湿度若低于40%时，环境相对是干燥的；若相对湿度高于60%时，环境相对是潮湿的。湿度过高过低对计算机的可靠性与安全性都有影响。当相对湿度超过65%以后，就会在元器件的表面附着一层很薄的水膜，会造成元器件各引脚之间的漏电，甚至可能出现电弧现象。当水膜中含有杂质时，它们会附着在元器件引脚、导线、接头表面，会造成这些表面发霉和触点腐蚀。磁性介质是多孔材料，在相对湿度高的情况下，它会吸收空气中的水分变潮，使其导磁率发生明显变化，造成磁介质上的信息读写错误。

在高湿度的情况下，打印纸会吸潮变厚，也会影响正常的打印操作。当相对湿度低于20%时，空气相当干燥，这种情况下极易产生很高的静电(实验测量可达10kV)，如果这时有人去碰MOS器件，会造成这些器件的击穿或产生误动作。过分干燥的空气也会破坏磁介质上的信息，会使纸张变脆、印刷电路板变形。如果对计算机运行环境没有任何控制，温度与湿度高低交替大幅度变化，会加速对计算机中的各种器件与材料的腐蚀与破坏作用，严重影响计算机的正常运行与寿命。计算机正常的工作湿度应该是40%～60%。

(3) 灰尘。

空气中的灰尘对计算机中的精密机械装置，如磁盘、光盘驱动器影响很大，磁盘机与光盘机的读头与盘片之间的距离很小，不到一个微米。在高速旋转过程各种灰尘，其中包括纤维性灰尘会附着在盘片表面，当读头靠近盘片表面读信号的时候，就可能擦伤盘片表面或者磨损读头，造成数据读写错误或数据丢失。放在无防尘措施空气中平滑的光盘表面经常会带有许多看不见的灰尘，即使用干净的布稍微用点力去擦抹，也会在盘面上形成一道道划痕。

如果灰尘中还包括导电尘埃和腐蚀性尘埃的话，它们会附着在元器件与电子线路的表面，此时机房若空气湿度较大的话，会造成短路或腐蚀裸露的金属表面。灰尘在器件表面的堆积，会降低器件的散热能力。因此，对进入机房的新鲜空气应进行一次或两次过滤，要采取严格的机房卫生制度，降低机房灰尘含量。

(4) 电磁干扰。

电气与电磁干扰是指电网电压和计算机内外的电磁场引起的干扰。常见的电气干扰是指电压的瞬间较大幅度的变化、突发的尖脉冲或电压不足甚至掉电。例如，计算机房内使用较大功率的吸尘器、电钻，机房外使用电锯、电焊机等大用电量设备，这些情况都容易

在附近的计算机电源中产生电气噪音信号干扰。这些干扰一般容易破坏信息的完整性,有时还会损坏计算机设备。防止电气干扰的办法是采用稳压电源或不间断电源,为了防止突发的电源尖脉冲,对电源还要增加滤波和隔离措施。

对计算机正常运转影响较大的电磁干扰是静电干扰与周边环境的强电磁场干扰。由于计算机中的芯片大部分都是 MOS 器件,静电电压过高会破坏这些 MOS 器件,据统计 50%以上的计算机设备的损害直接或间接与静电有关。

防静电的主要方法有:机房应该按防静电要求装修(如使用防静电地板),整个机房应该有一个独立的和良好的接地系统,机房中各种电气和用电设备都接在统一的地线上。周边环境的强电磁场干扰主要指可能的无线电发射装置、微波线路、高压线路、电气化铁路、大型电机、高频设备等产生的强电磁干扰。这些强电磁干扰轻则会使计算机工作不稳定,重则对计算机造成损坏。

2.1.3 硬件和基础设施安全的防护

1. 硬件安全的防护

硬件防护一般是指在计算机硬件(CPU、存储器、外设等)上采取的措施或者增加防护装置。如计算机加锁,加专门的信息保护卡(如防病毒卡、防拷贝卡),加插座式的数据变换硬件(如安装在并行口上的加密狗等),输入输出通道控制,以及用界限寄存器对内存单元进行保护等措施。

随着计算机技术的发展,超大规模集成电路的广泛应用使计算机的功能越来越完善,更新换代也越来越快。由于硬件安全防护措施的开支大,且不易随设备的更新换代而改变,因此,许多安全保护功能是由软件实现的。软件保护措施灵活,易实现、易改变,但它占用资源多、开销大,并且运行起来会降低计算机的性能。此外,完全依赖于软件的一些保密手段(如磁盘程序加密)易被软件破译,增加硬件防护才可保证安全可靠。因为上述原因,硬件防护措施仍是计算机安全防护技术中不可缺少的一部分。特别是对于重要的系统,需要硬件防护同系统软件的支持相结合,以保证安全。例如,虚拟存储器保护是一种硬件防护措施,但是其动态地址转换功能,需要有一套虚拟存储空间的表格结构,这需要操作系统支持。

(1) 存储器保护。

采用一对寄存器,将存储器区域保护属性存放在这对寄存器内,使存储器某区域的访问受到限制。这对寄存器就称为界限寄存器。界限寄存器提供保护的方法简单、可靠。由于界限寄存器对用户确定的存储区域并不为用户所知,因此,非法用户即使可以进入系统,但由于界限寄存器的保护,使他不知道要窃取信息的存放地点,并且它的保护范围也只限于界限寄存器规定的范围。这样就保护了信息的安全。界限寄存器原理如图 2-9 所示。

如图 2-9 所示,用寄存器 B_1、B_2 对用户 B 所使用的内存区进行保护(地址 20000~50000)。那么 B_1 中应该存放用户 B 使用内存的地址,即起始地址 20000;B2 中应该存放用户 B 使用内存连续存储区长度,即 30000。根据界限存储器 B_1、B_2 中的信息,中央处理

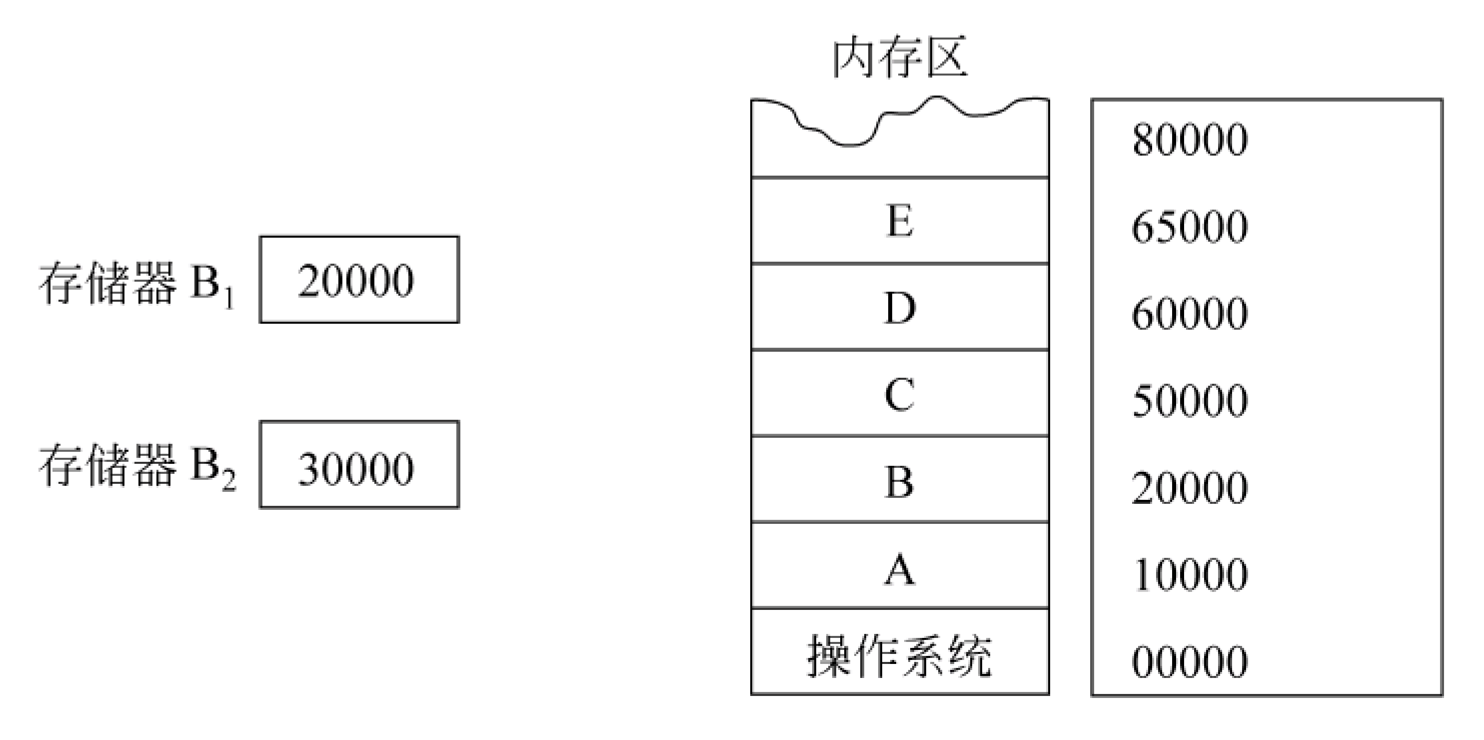


图 2-9　界限寄存器原理

器就可对重要信息实施有效保护。如果有另一个用户 A 要访问的信息或要调用的子程序在被保护的区域内，由于界限存储器的保护，A 就不能访问 B_1、B_2 所确定的区域。同样，用户 B 要超越界限去调用别的区域信息，也会受到限制。

(2) 虚拟存储保护。

虚拟存储是操作系统中的策略。当多用户共享资源时，为合理分配内存、外存空间，设置一个比内存大得多的虚拟存储器。用户程序和数据只是在需要时，才通过动态地址翻译并调用到内存(实存)中，供 CPU 调用，用后马上就退出。即内存中只存放执行时需要的程序段，其余程序和数据放在由虚拟的后备存储器内(磁盘上的一个区域)。程序不断执行，新的程序不断调入，而用过的程序段不断调出。周而往复，使内存的有限空间得到充分的利用。对用户而言，感到占用的是一个很大的虚拟存储器，并可根据虚拟存储器的地址编程，并不需要详细了解程序段的调入、调出过程，这个虚拟地址和实际地址的转换和调度过程是由操作系统来实现的。

虚拟存储保护应用较多的是段页式保护。段页式保护应用于段页式地址转换表格结构的虚拟存储器，如图 2-10 所示。虚拟地址分为虚段号、虚页号和页内地址，其中页内地址可直接转为实际地址，虚拟地址主要由段号和页号表示。段表在内存中的起始地址由段表基址寄存器和虚段号确定，虚段号为段表内地址位移量。段表基址与段号构成段表地址。而段表中的页表基址和虚页号又构成了页表地址。页表中实页号和虚拟地址中的页内地址构成了内存中的实际地址。

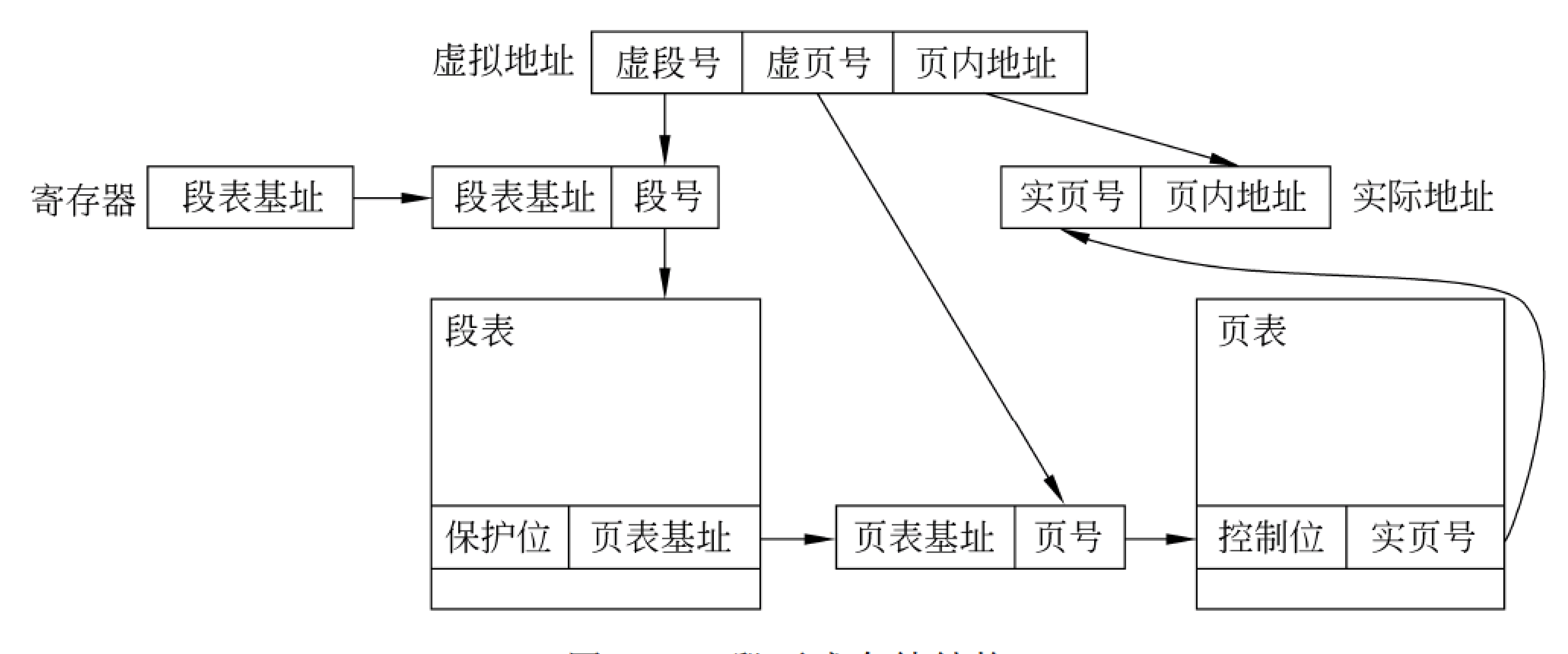


图 2-10　段页式存储结构

（3）输入输出通道保护。

输入输出过程是计算机系统运行中的重要环节之一，输入输出设备是计算机系统的重要组成部分。为使这一过程安全，要采取一定的措施来进行通道控制，这不仅可使系统安全保密，而且还可以避免由意外的操作失误而造成的损失。例如，对于键盘的输入，可采用键检测的方法对输入数据进行有效性的校核，可采用最后一位设置为校验位的方法，将前几位正确的输入值经过运算得到最后一位，通过检验最后一位来判断输入的正确性。

此外，针对输入输出特性，编写通道控制程序，说明更多的输入输出细节，并由输入输出控制器执行，使输入输出操作有更多的限制，从而保证通道安全。

2. 基础设施安全的防护

基础设施安全在整个计算机系统安全体系中占有重要地位。计算机系统基础设施安全的内涵是保护计算机系统设备、设施以及其他媒体设备免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。

基础设施安全保护内容可分为环境安全、设备安全、电源系统安全和通信线路安全。

（1）环境安全。

计算机系统的运行环境应按照国家有关标准设计实施，应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警，以保护系统免受水、火、有害气体、地震、静电等的危害。

（2）设备安全。

要保证硬件设备随时处于良好的工作状态，应当建立、健全使用管理规章制度，建立设备运行日志。同时要注意保护存储介质的安全性，包括存储介质自身和数据的安全。存储介质本身的安全主要是指安全保管、防盗、防毁和防霉；数据安全是指防止数据被非法复制和非法销毁等。

（3）通信系统安全。

通信设备和通信线路的装置安装要稳固牢靠，具有一定对抗自然因素和人为因素破坏的能力。它包括防止电磁信息的泄露、线路截获以及抗电磁干扰。

2.2 计算机硬件安全技术

计算机硬件安全是所有单机计算机系统和计算机网络系统安全的基础，计算机硬件安全技术是指用硬件的手段保障计算机硬件系统安全的各种技术。

本节主要介绍用硬件技术实现的 PC 防护技术、访问控制技术、可信计算和安全芯片技术与防电磁泄露技术。

2.2.1 PC 防护

1. 机箱锁扣

机箱锁扣实现的方式非常简单，如图 2-11 所示，在机箱上固定一个带孔的金属片，然

后在机箱钢板上打一个孔，当侧板安装在机箱上时，金属片刚好穿过锁孔，此时用户在锁孔上加装一把锁就实现了防护功能。

其特点是：实现简单，制造成本低。但由于这种方式防护强度有限，安全系数也较低。

2．Kensington 锁孔

Kensington 锁孔需要配合 Kensington 线缆锁来实现防护功能。Kensington 线缆锁由美国的 Kensington 公司发明，是一根带有锁头的钢缆，如图 2-12 所示。使用时将钢缆的一头固定在桌子或其他固定装置上，另一头将锁头固定在机箱上的 Kensington 锁孔内，就实现了防护功能。

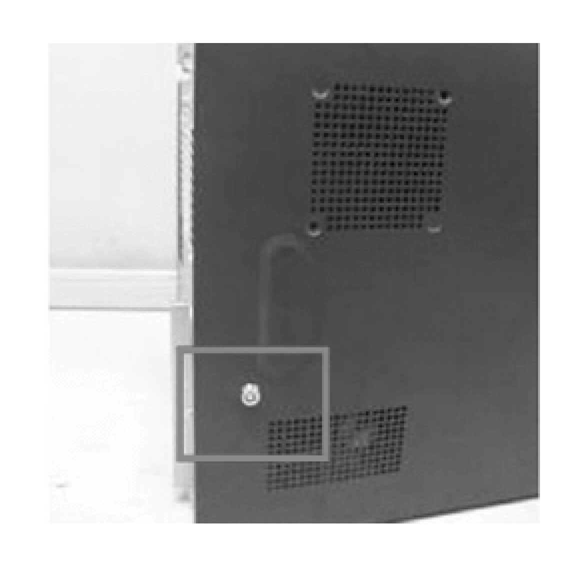


图 2-11　机箱锁扣



图 2-12　Kensington 锁

其特点是固定方式灵活，对于一些开在机箱侧板上的 Kensington 锁孔，不仅可以锁定机箱侧板，而且钢缆还能防止机箱被人挪走或搬走。

3．机箱电磁锁

机箱电磁锁主要出现在一些高端的商用 PC 产品上。如图 2-13 所示，这种锁是安装在机箱内部的，并且借助潜入在 BIOS 中的子系统通过密码实现电磁锁的开关管理，因此这种防护方式更加安全和美观，也显得更加人性化。

其特点是体现了较高的科技含量，但是也会带来整体采购成本的升高。

4．智能网络传感设备

如图 2-14 所示，将传感设备安放在机箱边缘，当机箱盖被打开时，传感开关自动复位，此时传感开关通过控制芯片和相关程序，将此次开箱事件自动记录到 BIOS（basic input output system，基本输入输出系统）中或通过网络及时传给网络设备管理中心，实现集中管理。

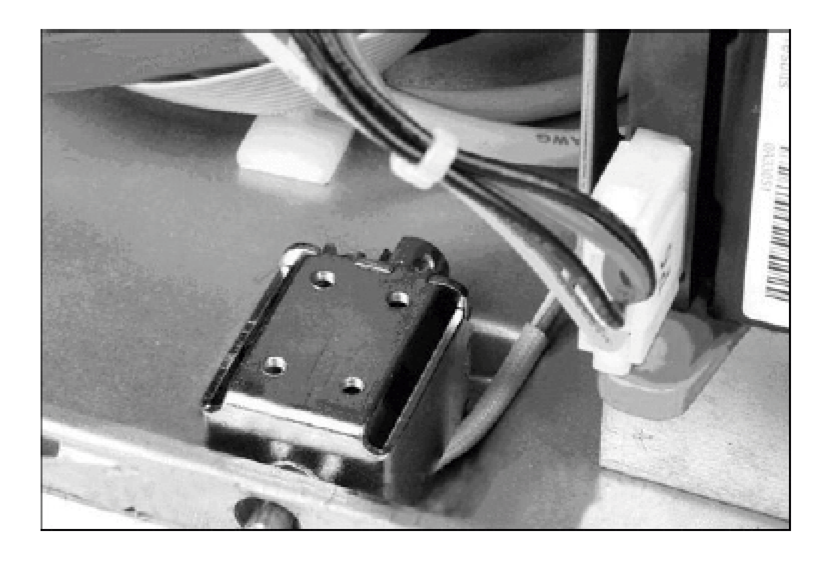


图 2-13　机箱电磁锁

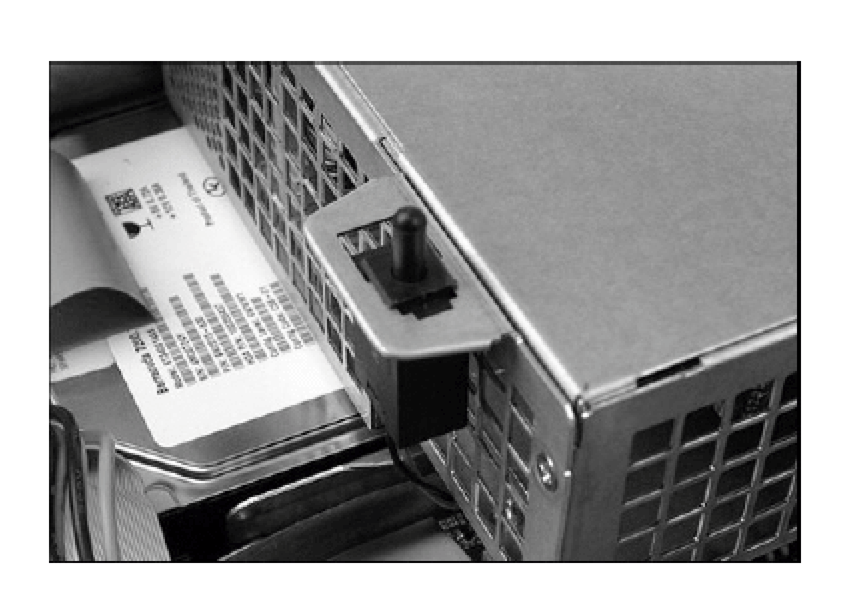


图 2-14　智能网络传感设备

其特点是：这是一种创新的防护方式。但是当网络断开或者计算机电源彻底关闭时，上述网络管理方式的弊端也就体现出来了。

上面四种只是品牌 PC 一些有代表性的物理防护方式，但实际上还有一些其他防护方式也常在商用 PC 上出现。如可以将键盘鼠标固定在机箱侧板上的安全锁、可覆盖主机后端接口的机箱防护罩等，这些都能从一定程度上保障设备和信息的安全。

5. 常用计算机硬件检测工具

利用计算机硬件检测软件对计算机硬件配置情况和使用情况进行检测是目前识别计算机硬件状况的主要手段，通过检测发现硬件存在的问题，可以更好地保护硬件的安全。

下面简单介绍几种比较常用的计算机硬件检测软件。

(1) 中央处理器信息检测(CPU-Z)。

CPU-Z 是一款家喻户晓的 CPU 检测软件，是检测 CPU 使用程度最高的一款软件，除了使用 Intel 或 AMD 自己的检测软件之外，用户使用最多的此类软件就数它了。CPU-Z 支持的 CPU 种类相当全面，软件的启动速度及检测速度都很快。另外，它还能检测主板和内存的相关信息，包括内存双通道检测功能。当然，CPU 的鉴别最好使用原厂软件。

(2) 系统检测分析工具(EVEREST)。

EVEREST(原名 AIDA32)一个测试软硬件系统信息的工具，它可以详细显示出 PC 每一个方面的信息。支持上千种(3400 多种)主板，支持上百种(360 多种)显卡，支持对并口/串口/USB 这些 PNP 设备的检测，支持对各式各样的处理器的侦测。

EVEREST Ultimate Edition 是最新的 EVEREST 超强力授权版，它比 EVEREST Home Edition、EVEREST Professional 等版本都要强大，也强过其他所有即时检测软件。它可以显示更多的项目，识别更多的新硬件和进行更多的测试，可在任务栏即时显示 5 项温度电压信息等。

(3) 360 硬件大师

360 硬件大师是一款非常不错的硬件检测工具，有温度监测、性能测试、一键电脑优化等功能，让用户即时了解自己计算机运行情况以及配置情况，值得一提的是，360 硬件大师为用户提供的温度实时监测工具栏，在屏幕的右下角显示，非常小巧，不占用屏幕空间，将鼠标移动到监测工具栏时将会显示更详细的监测情况，此项功能有助于用户做好计算机的降温工作。360 硬件大师是用户全面掌握计算机硬件配置的必备工具软件之一。

2.2.2 硬件访问控制技术

访问控制的对象主要是计算机系统软件与数据资源，这两种资源平时一般都是以文件的形式存放在硬盘或软盘上。所谓访问控制技术主要是指保护这些文件不被非法访问的技术。

由于硬件功能的限制，PC 的访问控制功能明显地弱于大型计算机。PC 操作系统设有提供有效的文件访问控制的机制。在 DOS 系统和 Windows 系统中，文件的隐藏、只读、只执行等属性以及 Windows 中的文件共享与非共享等机制是一种较弱的文件访问控

制机制。

PC 访问控制系统应当具备的主要功能有：

① 防止用户不通过访问控制系统而进入计算机系统。

② 控制用户对存放敏感数据的存储区域(内存或硬盘)的访问。

③ 对用户的所有 I/O 操作都加以控制。

④ 防止用户绕过访问控制直接访问可移动介质上的文件,防止用户通过程序对文件的直接访问或通过计算机网络进行的访问。

⑤ 防止用户对审计日志的恶意修改。

下面介绍常见的结合硬件实现的访问控制技术。

1. 令牌或智能卡

这里讲的令牌是一种能标识其持有人身份的特殊标志。例如,可以利用图章认证一个人的身份,公民身份证也是一种认证令牌。为了起到认证作用,令牌必须与持有人之间是一一对应的,要求令牌是唯一的和不能伪造的。身份证应该是不能伪造的,否则身份证就失去了意义。

各种磁卡,如邮政储蓄卡、电话磁卡等是用网络通信令牌的一种形式,这种磁卡后面记录了一些磁记录信息,通常磁卡读出器读出磁卡信息后,还要求用户输入通行字以便确认持卡人的身份。因此,如果磁卡丢失,拾到者也无法通过磁卡进入系统。还有一种更为复杂的信用卡形式——智能卡或芯片卡。这种卡中嵌入了一个微处理器。智能卡不仅可以保存用于辨别持有者身份的信息,还可以保存诸如存款余额的信息。这种卡不仅有存储能力,而且还有计算能力。

智能卡的使用过程大致如下：

一个用户在网络终端上输入自己的名字,当系统提示他输入通行字时,把智能卡插入槽中并输入其通行字,通行字不以明文形式回显,也不以明文方式传输,这是因为智能卡对它加密的结果。在接收端对通行字进行解密,身份得到确认后,该用户便可以进行他希望的网上操作了。

2. 生物特征认证方法

一般而言,生物统计学设备是用于保证某种安全有效和简单的设备。它可以测量与识别某个人的具体的生理特征,如指纹、声音、笔迹、打字手法或视网膜图像等特征。生物统计学设备通常用于极重要的安全场合,用于严格而仔细地识别人员身份。

(1) 指纹识别。

指纹识别技术是一种已经被接受的可以唯一识别一个人的方法。每个人都有唯一的指纹图像,把一个人的指纹图像保存在计算机中,当这个人想进入系统时,便将其指纹与计算机中的指纹匹配比较。有些复杂的系统甚至可以指出指纹是否是一个活着的人的指纹。

(2) 手印识别。

手印识别与指纹识别有所不同,手印识别器需要读取整个手而不仅是手指的特征图

像。一个人把他的手按在手印读入设备上,同时该手印与计算机中的手印图像进行比较。

(3) 声音。

每个人的声音都有细微的差别,没有两个人的声音是相同的。在每个人说话时都有唯一的音质和声音图像,甚至两个说话声音相似的人也是这样。识别声音图像的能力使人们可以基于某个短语的发音对人进行识别。声音识别技术已经商用化了,但当一个人的声音发生很大变化的时候(如患感冒),声音识别器可能会发生错误。

(4) 笔迹或签名。

分析某人的笔迹或签名不仅包括字母和符号的组合方式,还包括在书写签名或单词的某些部分用力的大小,或笔接触纸的时间长短和笔移动中的停顿等细微的差别。分析是通过一支生物统计学笔和板设备进行的,可将书写特征与存储的信息相比较。

(5) 击键分析。

文件打印出来后看起来是一样的,但它们被打印出来的方法是不一样的。这是击键分析系统的基础,该系统分析一个人的打字速度和节奏等细节特征。

(6) 视网膜识别技术。

视网膜识别技术是一种可用技术,但还没有像其他技术那样得到广泛的利用。视网膜扫描器用红外线检查人眼的血管图像,并和计算机中存储的图像信息比较。由于个人的视网膜是互不相同的,利用这种方法可以区别每一个人。由于害怕扫描设备出故障伤害人的眼睛,所以这种技术使用不广泛。

2.2.3 可信计算与安全芯片

1. 可信计算的核心思想

可信性(dependability)用来定义计算机系统的这样一种性质,即能使用户有理由认为系统所提供的各种服务确实是可以充分信赖的。

TCG(trusted computing group,可信计算组织)从行为角度来定义可信计算:如果一个实体的行为是可预期的,则称它是可信的。可信计算的核心思想是:构造“信任链”和“信任度量”的概念,如果从初始的“信任根”出发,在平台环境的每一次转换时,这种信任可以通过“信任链”传递的方式保持下去不被破坏,那么平台计算环境就始终是可信的。

2. 可信计算平台(TCP)

可信计算平台(trusted computing platform,TCP)是能够提供可信计算服务的计算机软硬件实体,它能够提供系统的可靠性、可用性和信息的安全性。可信计算平台以TPM(trusted platform module,可信平台模块)为信任根,为计算机系统信任验证提供了一种可行机制。

可信计算机系统由硬件平台、操作系统、应用程序、网络系统多个层次组成的。目前的 TCP 只是以 TPM 为核心提供了可信硬件平台。以可信 PC 平台为例,它以 TPM 为信任根,建立了 BIOS 引导块(bios boot block)→BIOS→OS 加载器(OS Loader)→OS 的信任链,将信任传递给了操作系统(OS)。真正的可信网络环境的构建,必须能保证信任

可传递到网络系统，一级认证一级，一级信任一级，从而把信任扩展到整个网络环境。也就是说，可信网络环境的构建必须需要安全操作系统、安全应用软件和安全网络系统等的一起配合才能真正实现。

3. 可信计算技术

可信计算技术通过在计算机中嵌入可信平台硬件设备，提供秘密信息硬件保护存储功能；通过在计算机运行过程中各个执行阶段(BIOS、OS 加载器、OS 等)加入完整性测量机制，建立系统的信任链传递机制；通过在操作系统中加入底层软件，提供给上层应用程序调用可信计算及服务的接口；通过构建可信网络协议和设计可信网络设备实现网络终端的可信接入问题。

由此可见，可信计算技术是从计算机系统的各个层面进行了安全增强，提供了比以往任何安全技术更加完善的安全防护功能，可信计算这个概念应用范畴已经包含从硬件到软件，从操作系统到应用程序，从单个芯片到整个网络，从设计过程到运行环境。随着网络的发展、计算的普及、计算环境的多元化，可信计算已经被提到空前的高度，引起了整个军事领域、学术界和产业界的高度关注。

与传统的安全技术相比，可信计算技术具有以下三个显著的功能特征。

(1) 保护存储(protected storage)。

保护存储一方面通过嵌入的设备保护用户特定的秘密信息(如终端平台身份信息、密钥等)，防止通过硬件物理窥探等手段访问密钥等信息；另一方面完成硬件保护下的密钥生成、随机数生成、Hash 运算、数字签名以及加密操作，为用户提供受保护的密码处理过程。

(2) 认证启动(authenticated boot)。

可信计算技术利用完整性测量机制完成计算机终端从加电到操作系统装载运行过程中各个执行阶段的认证。当低级别的节点认证到高一级的节点是可信时，低级别节点会把系统的运行控制权转交给高一级节点，基于这种信任链传递机制，可以保证终端始终处于可信的运行环境中。

(3) 证明(attestation)。

证明是保证信息正确性的过程。网络通信中，计算机终端基于数字证书机制可以想要通信的对方证明终端当前处于一个可信状态，同时说明本机的配置情况。如果通信双发都能证明彼此信息的有效性，则可以继续进行通信，否则服务中断。

基于以上三个功能特征，可信计算技术可以对主机实施有效的安全防护，保护计算机及网络系统的安全运行，从而向用户提供一个可信的执行环境。

4. 基于安全芯片的可信计算机

TCG 定义了具有安全存储和加密功能的 TPM，并于 2001 年 1 月 30 日发布了基于硬件系统的“可信计算平台规范”1.0 版标准。该标准通过在计算机系统中嵌入一个可抵制篡改的独立计算引擎，使非法用户无法对其内部的数据进行更改，从而确保了身份认证和数据加密的安全性，2003 年 10 月发布了 1.2 版标准。

TPM 的核心是含有密码运算部件和存储部件的小型芯片系统(system on chip，SOC)，由 CPU、存储器、I/O、密码运算器、随机数产生器和嵌入式操作系统等部件组成，称为 TPM 的安全芯片。

TPM 芯片的功能在于对 CPU 处理的数据流进行加密，同时检测系统底层的状态。在这个基础上，可以开发出唯一身份识别、系统登录加密、文件夹加密、网络通信加密等各个环节的安全应用，它能够生成机密的密钥，还有密钥的存储和身份的验证，可以高速进行数据加密和还原，作为呵护 BIOS 和操作系统不被修改的辅助处理器，通过可信计算软件栈 TSS 与 TPM 的结合来构建跨平台与软硬件系统的可信计算体系结构。用户即使硬盘被盗，由于缺乏 TPM 的认证处理，不会造成数据泄露。目前国内一些厂商已经将 TPM 芯片应用到台式机领域。图 2-15 分别为贴有 TPM 标志的主机箱(见右下角)、兆日公司的 TPM 芯片及在主板上的状态。



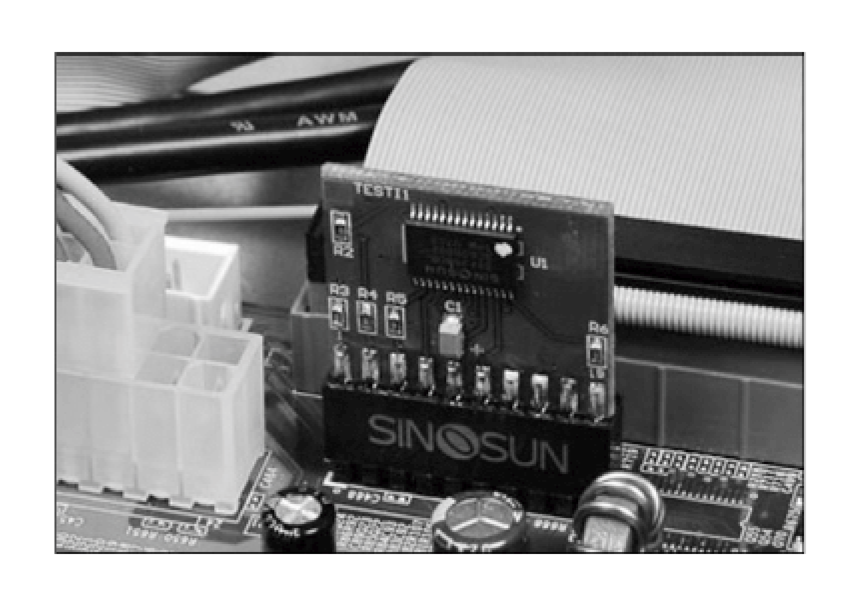


图 2-15　TPM 主机箱和芯片

要想查看计算机是否有 TPM 芯片，可以打开“设备管理器”，查看其中是否存在“安全设备”节点，该节点下是否有“受信任的平台模块”这类设备，并确定其版本即可，如图 2-16 所示。



图 2-16　TPM 设备查看

以 TPM 为基础的可信计算机主要有以下三个安全功能。

(1) 用户的身份认证，这是对使用者的信任。传统的方法是依赖操作系统提供的用户登录，这种方法具有两个致命的弱点，一是用户名称和密码容易仿冒，二是无法控制操

作系统启动之前的软件装载操作，所以被认为是不够安全的。而可信计算平台对用户的鉴别则是与硬件中 BIOS 相结合，通过 BIOS 提取用户的身份信息，如 IC 卡或 USB KEY 中的认证信息进行验证，从而让用户身份认证不再依赖操作系统，并且用户身份信息的假冒更加困难。

（2）可信计算平台内部各元素之间互相认证，体现了使用者对平台运行环境的信任。系统的启动从一个可信任源（通常是 BIOS 的部分或全部）开始，依次将验证 BIOS、操作系统装载模块、操作系统等，从而保证可信计算平台启动链中的软件未被篡改。

（3）平台之间的可验证性，指网络环境下平台之间的相互信任。可信计算平台具备在网络上的唯一的身份标识。现有的计算机在网络上是依靠不固定的 IP 地址进行活动，导致网络黑客泛滥和用户信息不足。具备由权威机构颁发的唯一身份证书的可信计算平台，则可以精确地提供自己的身份认证，从而为电子商务之类的系统应用奠定信用基础。

2.2.4　硬件防电磁泄漏

俗话说“明箭好躲，暗箭难防”，主要是讲人们在考虑问题时常常会对某些可能发生问题的某些方面估计不足，缺少防范心理。在考虑计算机安全问题的时候，往往也存在这种情况，一些用户常常仅会注意计算机内存、硬件、软盘上的信息泄露问题，而忽视了计算机通过磁辐射产生的信息泄露。一般把前一类称为信息的“明”泄露，后一类的信息泄露称为信息的“暗”泄露。

1. 防信息辐射泄漏技术

计算机是一种非常复杂的机电一体化设备，工作在高速脉冲状态的计算机就像是一台很好的小型无线电发射机和接收机，不但产生电磁辐射泄露保密信息，而且还可引入电磁干扰影响系统正常工作。尤其是在微电子技术和卫星技术飞速发展的今天，计算机电磁辐射泄密的危险越来越大。

国际上把防信息辐射泄露技术简称为 TEMPEST（transient electromagnetic pulse emanations standard technology）技术，这种技术主要研究和解决计算机和外部设备在工作时因电磁辐射和传导所产生的信息外露问题。TEMPEST 的主要研究范围包括理论、工程和管理等方面，涉及电子、电磁、测量、信号处理、材料和化学等多学科的理论与技术。

TEMPEST 的研究内容主要有以下几个方面：

（1）电子信息设备是如何让辐射泄漏的——研究电子设备辐射的途径与方式，研究设备的电气特征和物理结构对辐射的影响。

（2）电子信息设备辐射泄漏如何防护——研究设备整体结构和各功能模块的布局、系统的接地、元器件的布局与连线以及各种屏蔽材料、屏蔽方法与结构的效果等问题。

（3）如何从辐射信息中提取有用信息——研究辐射信号的接收与还原技术。由于辐射信号弱小、频带宽等特点，需要研究低噪声、宽频带、高增益的接收与解调技术，进行信号分析和相关分析。

（4）信息辐射的测试技术与测试标准——研究测试内容、测试方法、测试要求、测试仪器以及测试结果的分析方法，并制定相应的测试标准。

2. 信息设备的电磁泄漏威胁

信息设备是信息技术设备和处理信息的模拟设备的总称。按麦克斯韦电磁理论，在电磁波的空间某处有电荷的加速运动，或电流随时间变化所引起的扰动会向四周传播。信息设备微弱的电流变化都会产生电磁场的发射。如果该电磁发射是由红信号（携带涉密明文信息的信号为红信号，否则称为黑信号）的电流变化引起的，则被称为电磁泄漏发射。

理论分析表明，泄漏发射强度和电路中的变化程度成正比。现今大部分信息设备的红信号是数字信号，数字信号电平的大小和沿的陡峭程度（越陡峭意味着电流变化越快）决定了发射强度的高低。因此，随着信息技术设备处理速度的不断提高，电磁发射强度也会不断增强，对信息安全的威胁也会越来越大。

信息设备的电磁泄漏发射分为辐射和传导两种方式。辐射发射是信息设备电磁波在自由空间的传播，辐射发射如同广播电视发射信号，可被天线和接收机接收处理。通过金属导体（例如电源线和通信线）或任何金属结构的传播构成了信息设备的传导发射，可通过电流卡钳等感应导体电流变化的设备截取到。

信息设备的电磁泄漏分为以下几种类型。

（1）计算机系统的电磁泄漏。

① 计算机及外设产生的电磁泄漏，伴随信息的接收、处理和发展的全过程，包括视频信息、键盘输入信息、磁盘信息等计算机处理数据。泄漏发射源包括显示器、键盘、软驱、主板及各种连接电缆接口等。从信息的传输方式分为串行信号的泄漏和并行信息的泄漏。计算机系统中并行信号泄漏发射之间形成同频相关干扰。从中提取红信号十分困难。对信息威胁最大的是串行信号的泄漏发射。产生串行信号的部件有显示器、键盘、软驱、RS 232 通信线等。

② 其他信息设备的电磁泄漏。如电话机、打印机、复印机和传真机处理信息的方式都是以串行为主。它们的电磁泄漏同样具有威胁。

（2）声光的泄漏威胁。

除了电流引起的电磁泄漏发射对信息安全造成威胁外，声音和光的无意识泄漏也会造成信息的泄露。

① 光的泄漏威胁。如果计算机显示器直接面对窗外，它发出的光可以在直线很远的距离上接收到。即使没有直接的通路，接收显示器通过墙面发射的光线仍然能再显示屏幕信息。这种光泄漏和电磁泄漏异曲同工，在目前复杂的电磁环境下，光信号的接收还原是很容易实现的。

② 声音信号也存在泄漏现象。例如，通过点阵式打印机击打打印纸发出的声音能够复原出打印的字符。美国有关 TEMPEST 的资料中，也有降低点阵式打印机噪声的要求。

3. 防泄漏措施

对计算机与外部设备究竟要采取哪些防泄漏措施，要根据计算机中信息的重要程度而定。对于企业而言，需要考虑这些信息的经济效益，对于军队则需要考虑这些信息的保

密级别。在选择安全措施时，不应该花费 100 万元去保护价值 10 万元的信息。

下面介绍一些常用的防泄漏措施。

（1）整体屏蔽。

屏蔽不但能防止电磁波外泄，而且还可以防止外部的电磁波对系统内设备的干扰。

对军队、政府机关、科研院所 、学校等要害部门的一些办公室、实验场所，甚至整栋大楼用昂贵的有色金属网或金属板进行屏蔽，构成所谓的“法拉第笼”，并注意连接的可靠性和接触良好，防止向外辐射电磁波，避免外面的电磁干扰系统内的设备。

另外，因为计算机系统工作时，除了以电磁波方式辐射电磁能量以外，还可以通过电源线、信号线和地线等以传导的方式泄漏，因此同时也要加强对整个电子设备的屏蔽，如对显示器、键盘、传输电缆线、打印机等的整体屏蔽，对电子线路中局部器件，如有源器件、CPU、内存条、字库、传输线等强辐射部位采用屏蔽盒、合理布线等，以及局部电路的屏蔽。一台符合 TEMPEST 防护标准的计算机，它的结构、机箱、键盘、显示器与普通计算机在外观上会有明显的不同。

整个房间屏蔽的费用比较高，如果用户承担不起，可以采用设备屏蔽的方法，把需要屏蔽的计算机和外部设备放在体积较小的屏蔽箱内，该屏蔽箱要有很好的接地。对于从屏蔽箱内引出的导线也要套上金属屏蔽网。

（2）隔离和安全布局。

隔离和安全布局均为降低电磁泄漏的有效手段。隔离是将信息系统中需要的重点防护的设备从系统中分离出来，加以特别防护，并切断与系统中其他设备间的电磁泄漏通路。

安全布局是指以减少电磁泄漏为原则，安全地放置信息系统中的有关设备。安全布局也包括尽量拉大涉密设备与非安全区域(公共场所)的距离。可以让计算机机房远离可以被侦测的地点，因为计算机辐射有一定的距离限制。对于一个单位而言，计算机机房尽量建在单位辖区的中央地区。若一个单位辖区的半径少于 300m，距离防护的效果就有限。

此外即使在屏蔽室内，也必须把红、黑设备隔离。其中红设备是指有信息泄露危险的元器件、部件和连线等设备，黑设备是指处理、传输非保密数据的设备。如果要连接红、黑设备，必须要通过严格的 TEMPEST 测试，按照规范进行连接。

（3）滤波器与铁氧体磁环。

滤波是抑制传导泄漏的主要方法之一。电源线或信号线上加装合适的滤波器，可以阻断传导泄漏的通路，从而大大抑制传导泄漏。

在屏蔽的电缆线的两端套上铁氧体磁环可以进一步减少电缆的辐射强度。

（4）接地和搭接。

接地和搭接也是抑制传导泄漏的有效方法。良好的接地和搭接，可以给杂散电磁能量一个通向大地的低阻回路，从而在一定程度上分流掉可能经电源线和信号线传播出去的电磁能量。用这一方法和屏蔽、滤波等技术配合使用，对抑制电子设备的电磁泄漏可起到事半功倍的效果。

（5）使用干扰器。

干扰器是一种能辐射出电磁噪声的电子仪器。它是通过电磁噪声降低辐射泄露信息

的总体信噪比，增大辐射信息被截获后破解还原的难度，从而达到“掩盖”真实信息的目的。其防护的可靠性也相对较差，因为设备辐射出的信息量并未减少。从原理上讲，运用合适的信息处理手段，仍有可能还原出有用信息，只是还原的难度相对增大。这是一种成本相对低廉的防护手段，主要用于保护密级较低的信息。此外，使用干扰器还会增加周围环境的电磁污染，对其他电磁兼容性较差的电子信息设备的正常工作构成一定的威胁。所以只能在没有其他有效防护手段的前提下，作为应急措施才使用干扰器。

(6) 配置低辐射设备。

低辐射设备是在设计和生产计算机时就已对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取了防辐射措施。它和屏蔽手段相结合使用可以有效地保护绝密级信息。例如，可以采用低辐射的液晶显示器来代替高辐射的 CRT 显示器。

(7) 软件 TEMPEST 防护技术。

TEMPEST 防护技术从 20 世纪 60 年代就开始了，现在其技术已经逐渐成熟。不过一台符合 TEMPEST 防护标准的计算机的造价非常昂贵，通常是普通计算机的五倍。一间几十平方米的屏蔽室的成本少则几十万元，甚至好几百万。这给对电磁辐射的防护工作带来了一定的困难。

软件 TEMPEST 是近几年兴起的用计算机软件控制信息泄露的新技术。针对的保密信息主要是文字、数字信息，防止信息泄露就是如何防止这些文字信息被别人窃取，TEMPEST 字体是一种有效的防止文字信息泄露的新方法。经过特殊处理的 TEMPEST 字体即使被 TEMPEST 供给设备截获，也根本无法还原泄露信息的内容。

(8) TEMPEST 测试技术。

TEMPEST 测试技术即检验电子设备是否符合 TEMPEST 标准。其测试内容并不限于电磁发射的强度，还包括对发射信号内容的分析、鉴别。

(9) SOFT-TEMPEST 技术。

SOFT-TEMPEST 技术是由英国剑桥大学两位学者于 1997 年发明并推广应用的一项防信息泄漏新技术，其基本原理是通过给视频字符添加高频“噪声”并伴随发射伪字符，使敌方无法正确还原真实信息，而我方可正常显示，质量无变化，它替代了过去由硬件完成的抑制干扰功能，成本较低。采用 TEMPEST 技术的防护型 TEMPEST 计算机，使用软件来控制计算机机密信号的发射，同时加入了专用的攻击程序，当有人企图截获信息时系统能自动保护并进行自卫反击。

2.3 基础设施与环境安全

基础设施和环境的安全严重影响着计算机系统的安全，其中计算机机房的安全是重中之重，本节主要介绍计算机机房及环境安全，并简要概述其他基础设施安全以及设备和通信线路安全。

2.3.1 计算机机房及环境安全

为了确保计算机硬件和计算机中信息的安全，机房安全是重要的因素。本节将讨论

有关机房的安全问题。先讨论机房的安全等级，然后再讨论机房对场地环境的要求。

1. 计算机机房安全等级

计算机系统中的各种数据依据其重要性和保密性，可以划分为不同的等级，需要提供不同级别的保护。对于高等级数据采取低水平的保护会造成不应有的损失，对不重要的信息提供多余的保护，又会造成不应有的浪费。因此，应对计算机机房规定不同的安全等级。根据国标 GB 9361—88《计算站场地安全要求》，计算机机房的安全等级分为三级，A 级要求具有最高安全性和可靠性的机房；C 级是为确保系统作一般运行而要求的最低限度的安全性、可靠性的机房；介于 A 级和 C 级之间的则是 B 级。计算机安全等级的划分如表 2-1 所示。

表 2-1　机房的安全等级

安全项目 \ 指标 \ 机房安全级别	C	B	A	安全项目 \ 指标 \ 机房安全级别	C	B	A
场地选择	－	＋	＋	防水	－	＋	⊕
防火	＋	＋	＋	防静电	－	＋	⊕
内部装修	－	＋	⊕	防雷击	－	＋	⊕
供配电系统	＋	⊕	⊕	防鼠害	－	＋	⊕
空调系统	＋	⊕	⊕	电磁波的防护	－	＋	＋
火灾报警及消防设施	＋	＋	⊕				

表中符号的说明：－　无须要求；＋　有要求或增加要求；⊕　要求。

应该根据所处理信息及运用场合的重要程度来选择适合本系统特点的相应安全等级的机房，而不应该要求一个机房内的所有设施都达到某一安全等级的要求。可以按不同级别的要求建设机房。例如，有些系统可根据处理信息的实际情况将数据保护的安全措施定位 A 级，把电源系统定位 B 级，火灾报警及消防措施定位 C 级。

2. 计算机机房环境安全基本要求

计算机系统的实体是由电子设备、机电设备和光磁材料组成的复杂系统。这些设备的可靠性和安全性与环境条件有着密切的关系。如果环境条件不能满足设备对环境的要求，就会降低计算机的可靠性和安全性，轻则造成数据或程序的出错、破坏，重则加速元器件老化，缩短计算机的寿命，或发生故障使系统不能正常运行，严重时还会危害设备和人员安全。

(1) 机房外部环境要求。

机房场地的选择应以能够保证计算机长期稳定、可靠、安全地工作为主要目标。在外部环境的选择上，应考虑环境安全性、地质可靠性、场地抗电磁干扰性，应避开强振动源和强噪声源，应避免设在建筑物的高层以及用水设备的下层或隔壁。

同时，应尽量选择电力、水源充足，环境清洁，交通和通信方便的地方。对于机要部门

信息泄露，机房最好建设在单位的中央地区。

（2）机房内部环境要求。

① 机房应辟为专用和独立的房间；

② 经常使用的进出口应限于一处，以便于出入管理；

③ 机房内应留有必要的空间，其目的是确保灾害发生时人员和设备的撤离和维护；

④ 机房应设在建筑物的最内层，而辅助区、工作区和办公房设在其外围。A、B级安全机房应符合这样的布局，C级安全机房则不作要求。

（3）机房面积要求。

机房面积的大小与需要安装的设备有关，另外还要考虑人在其中工作是否舒适。通常有两种估算方法，一种是按机房内设备总面积 M 计算。计算公式如下：

$$\text{机房面积} = (5 \sim 7)M$$

这里的设备总面积是指所有设备的最大外形尺寸的总和，如所有的计算机、网络设备、I/O设备、电源设备、资料柜、耗材柜、空调设备等。系数5～7是根据现有机房的实际使用面积和设备所占面积之间关系的统计数据确定的，实际应用时根据本单位具体情况进行调整。

第二种方法是根据机房内设备的总数进行机房面积估算。若设备的总台数为 K，则估算公式为：

$$\text{机房面积} = (4.5 \sim 5.5)K$$

在这种计算方法中，估算的准确与否和各种设备的尺寸是否大致相同有密切关系，一般的参考标准是按台式计算机的尺寸为一台设备进行估算。如果一台设备占地面积太大，最好把它按两台或多台台式计算机去计算，这样可能更会准确。系数4.5～5.5也是根据我国具体情况的统计参数。

2.3.2 设备安全

计算机信息系统的硬件设备一旦被破坏又不能及时修复，不仅会造成经济损失，而且可能导致整个系统瘫痪，产生严重的后果。因此，必须加强对计算机信息系统的硬件设备的使用管理，坚持做好硬件设备的日常维护和保养工作。

1. 硬件的使用管理

（1）根据硬件设备的具体配置情况，制定切实可用的硬件设备操作使用规程，并严格按照此规程对硬件设备进行操作。

（2）建立设备使用日志，对使用过程中的情况进行严格登记。

（3）建立设备故障情况登记表，对故障性质和修复情况进行详细记录。

（4）对设备进行定期的维护和保养，可以指定专门负责人。

2. 常用硬件设备的维护和保养

常用硬件设备的维护和保养的相关内容将在2.5节具体实例中提到，这里不作叙述。另外，在硬件设备的使用说明书上也有该设备的维护和保养说明。

3. 信息存储介质的安全管理

计算机系统的信息存储在某种存储介质上，常用的存储介质有磁带、硬盘、光盘、打印纸等。对存储介质的安全管理主要包括以下几个方面。

（1）存放有业务数据或程序的磁盘、磁带或光盘，应妥善保管，必须注意防磁、防潮、防火和防盗。

（2）对硬盘上的数据，要建立有效的级别、权限，并严格管理，必要时要对数据进行加密，以确保硬盘的安全。

（3）对存放业务数据或程序的磁盘、磁带或光盘，管理必须落实到人；对存放有重要信息的磁盘、磁带、光盘，要备份并分两处保管。

（4）带有业务数据的打印纸，要视同档案进行管理。

（5）对需要进行长期保存的数据，应在存储介质的质量保证期内进行转存，存储时应确保内容正确。

（6）对超过数据保存期的存储介质，必须进行特殊的数据清除工作。

2.3.3 通信线路安全

尽管从网络通信线路上提取信息所需要的技术比直接从通信终端获取数据的技术要高几个数量级，不过，以目前的技术水平也是完全有可能实现的。

1. 加压电缆线路

要实现通信线路上的物理安全可以使用一种简单（但很昂贵）的高技术加压电缆。该技术原是为美国国家电话系统开发的。通信电缆密封在塑料套管中，并在线缆的两段充气加压。线上连接了带有报警器的监视器，用来测量压力。如果压力下降，则意味电缆可能被破坏了，技术人员还可以进一步检测出破坏点的位置，以便及时进行修复。

电缆加压技术提供了安全的通信线路。将加压电缆架设于整座楼中，每寸电缆都将暴露在外。如果任何人企图割电缆，监视器会启动报警器，通知安全保卫人员电缆已被破坏。假设任何人成功地在电缆上接了自己的通信线路，在安全人员定期地检查电缆的总长度时，就可以发现电缆拼接处。加压电缆是屏蔽在波纹钢丝网中的，几乎没有电磁辐射，从而大大增强了通信线路窃听的难度。

2. 光纤通信线路

因为光纤通信线发生破断会被检测到，同时线路上拼接处的传输速度会缓慢得令人难以忍受，所以光纤通信线曾被认为是不可搭线窃听的。而光纤也没有电磁辐射，所以也不能用电磁感应窃密。不幸的是，光纤的最大长度有限制，目前光纤的网络覆盖范围半径约 100km，大于这一长度的光纤系统必须定期地放大（复制）信号。这就需要将信号转换成电脉冲，然后再恢复成光脉冲，继续通过另一条线路传送。完成这一操作的设备，即复制器，是光纤通信系统的安全薄弱环节，因为信号可能在这一环节被搭线窃听。有两个办法可解决这一问题：距离大于最大长度限制的系统之间，不采用光纤通信或加强复制器的安全，如用加压电缆、警报系统和加强警卫等措施。

2.4 硬件故障及维护应用实例

计算机在给用户带来极大方便的同时，也给用户带来不少烦恼——运行缓慢，经常死机，无故重启，硬盘故障，显示器无法显示等。其实计算机并不像用户想象得那么神秘，只要用户了解计算机硬件和常用外设的故障排除方法，掌握“治病良方”就可以使计算机更好地为用户所用。

本节将通过应用实例介绍一款系统检测分析工具的使用，介绍一些计算机系统常见的故障与计算机硬件和常用外设故障的排查方法。

2.4.1 使用 EVEREST 进行系统检测

系统检测分析工具 EVEREST(原名 AIDA32)是一个测试软硬件系统信息的工具软件，它可以详细地显示出 PC 每一个方面的信息。支持上千种(3400 多种)主板，支持上百种(360 多种)显卡，支持对并口/串口/USB 这些 PNP 设备的检测，支持对各式各样的处理器的侦测。

下面介绍使用 EVEREST 进行系统检测的方法。

1. 下载并安装软件

在 EVEREST 的官方网站上下载 EVEREST Ultimate Edition v5.50(.EXE)，单击安装文件，根据需要选择相应语言，如图 2-17 所示。



图 2-17 选择安装语言

2. 查看安装后的软件

安装完成后，会自动跳转到 EVEREST 主界面，如图 2-18 所示。

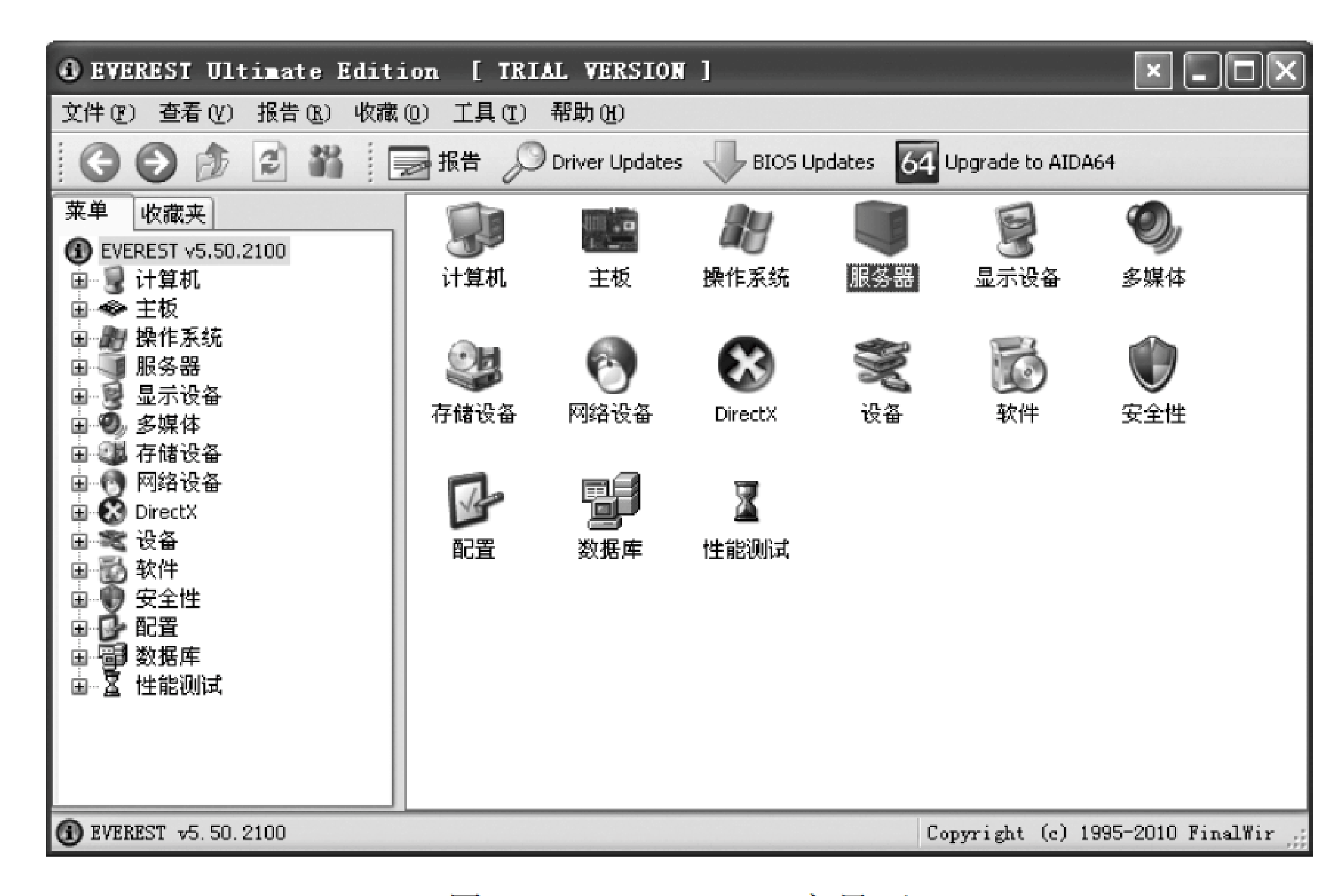


图 2-18 EVEREST 主界面

通过上面的界面可以看到，这款软件是一款几乎包容所有计算机信息的软件。

3. 建立计算机信息报告

EVEREST 可以帮助用户建立计算机信息报告，用户可以选择某部分创建报告，例如，可以创建硬件相关的信息报告，也可创建计算机全部的信息。报告的生成格式也是多种多样的，例如 TXT 纯文本或者 HTML 等。

建立硬件信息报告的步骤如下：

（1）在工具栏单击【报告】按钮，打开“本地报告向导”，如图 2-19 所示。



图 2-19 “本地报告向导”欢迎界面

（2）单击【下一步】按钮，本界面用来选择“报告配置文件”，这里仅选择“硬件相关内容”，如图 2-20 所示。



图 2-20 “本地报告向导”报告配置文件界面

(3) 单击【下一步】按钮，进入选择“报告格式”界面，这里选择 HTML 格式，如图 2-21 所示。



图 2-21 “本地报告向导”报告格式界面

(4) 单击【完成】按钮，将自动生成计算机硬件信息报告，如图 2-22 所示。

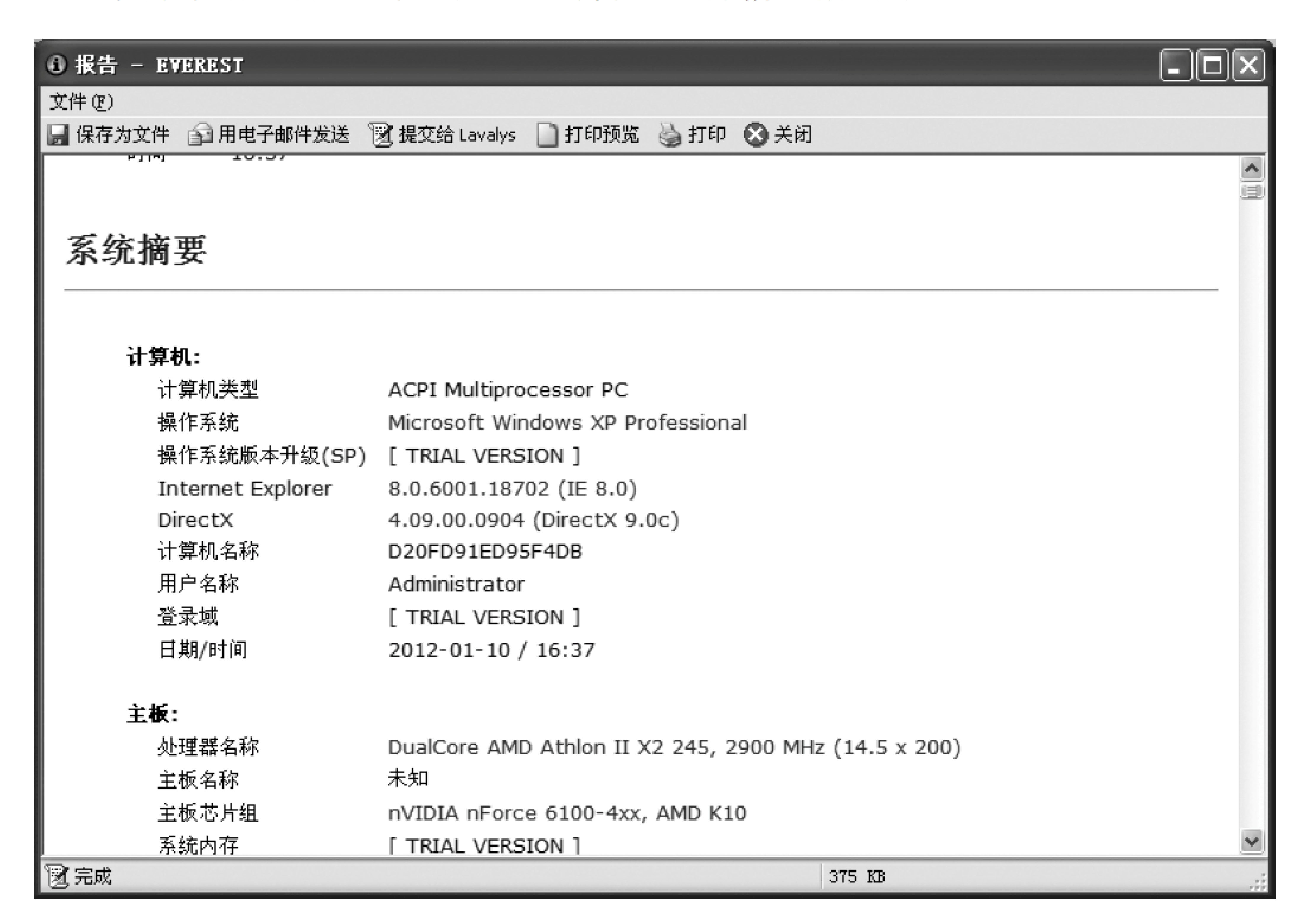


图 2-22 计算机硬件信息报告

4. 查看系统信息

通过单击主界面右侧菜单栏中的选项即可查看系统各项信息，此操作较简单在这里就不再赘述。

EVEREST 这款软件具有非常强大的功能，既可以实时检测计算机的软硬件信息，又可以进行基准测试，查看系统性能，还可以通过插件功能进行更专业化的测试。

2.4.2 主板常见故障及维护

1. 主板故障排查的常用方法

当主板出现故障时，一般会导致系统无法正常启动、屏幕无显示等现象。对主板故障进行排查的方法主要有以下几种。

(1) 清洁法。使用较软的刷子将主板上的灰尘刷去；对主板上的各个插槽进行擦拭，并轻轻地擦拭主板上的内存、显卡的金手指。

(2) 观察法。查看主板上的原件是否有烧毁，检查各插头、插座是否歪斜，电容、电阻引脚是否相碰。如果发现存在上述问题，可以借助万用表测量一下。触摸一些元件的表面，检查其是否过热，如果过热则更换新的元件。

(3) 插拔法。根据开机时的报警铃声来判断哪个元件发生了问题，然后将可能的元件进行更换，从而判断到底是哪个元件出了问题。

(4) 软件诊断法。通过随机附带的诊断程序、维修诊断卡等软件来诊断故障，一般检查电路故障。

这些方法有各自的优势和局限 ，应结合使用。

2. 无法正确识别键盘和鼠标

出现这种故障的原因可能是：主板不支持鼠标、键盘，系统无法找到鼠标键盘，即使可以找到鼠标，鼠标操作也不受控制；或者键盘、鼠标与计算机连接时，出现接口连接松动现象，这样就会很容易造成键盘、鼠标与主板接触不良；还有一种原因，就是鼠标、键盘本身有故障，导致系统无法识别，解决此问题步骤如下：

(1) 查看主板说明书，看当前使用的鼠标、键盘是否与主板兼容，如不兼容，重新更换主板可以兼容的鼠标、键盘即可。

(2) 检查鼠标、键盘的连接端口，看是否松动，如果有松动可重新更换鼠标、键盘的接口，确保连接稳定、可靠。

(3) 如果还不能解决，则检查鼠标、键盘本身，查看它们的供电电压是否为＋5V，若不正常，检查供电保险丝是否出现熔断现象，如果保险电阻数值很大的话可用细导线直接连通。

3. 计算机频繁死机

计算机频繁死机，在进行 CMOS 设置时也会出现死机现象。此类故障一般是由于主板 cache(缓存)有问题或主板散热不良引起的，解决此问题步骤如下：

(1) 死机后触摸 CPU 周围的主板的元器件，如果发现其温度非常高，应尽快更换大功率风扇。

(2) 如果更换风扇后故障依然存在，那就是主板 cache 有问题了，可以在 COMS 中将 cache 关掉。

(3) 重启计算机,按 Del 键进入 BIOS 主程序,选择 BIOS FEATURES SETUP 选项,然后按 Enter 键进入。

(4) 选择 External Cache 选项,将参数由 Enabled 改为 Disabled,即可关闭主板上的 Cache,如图 2-23 所示。

CMOS Setup Utility - Copyright (C) 198
Advanced BIOS Feat

Virus Warning	[Disabled]
CPU Internal Cache	[Enabled]
External Cache	[Enabled]
CPU L2 Cache ECC Checking	[Disabled]

图 2-23 将 Enabled 改为 Disabled

4. 系统时间老是自动变慢

每次开机后,计算机系统时间都会比正常时间慢,重新设定好之后下一次开机又会变慢。该故障是由于主板 COMS 电池电量不足或石英晶体故障引起的,解决此问题步骤如下:

(1) 更换一个新的主板 COMS 电池,如图 2-24 所示。

(2) 若故障依然存在,则有可能是石英晶体工作不稳定或已经损坏。可用无水酒精清洁计时电路附近的电路板,若故障仍没有排除,则需要更换石英晶体。

5. 计算机连续发出"嘀嘀"声

计算机开机后无任何显示,并连续发出"嘀嘀"的报警声。

根据报警声提示,可判断为内存故障。此类故障一般是由于内存条的金手指制作工艺差,表面镀金不良,长期使用后表面的氧化层增厚,导致内存和主板接触不良,解决此问题步骤如下:

(1) 打开机箱,取下内存条,用橡皮擦将内存条的金手指擦拭干净。

(2) 将擦拭干净的内存条重新插上,计算机即可正常工作,如图 2-25 所示。

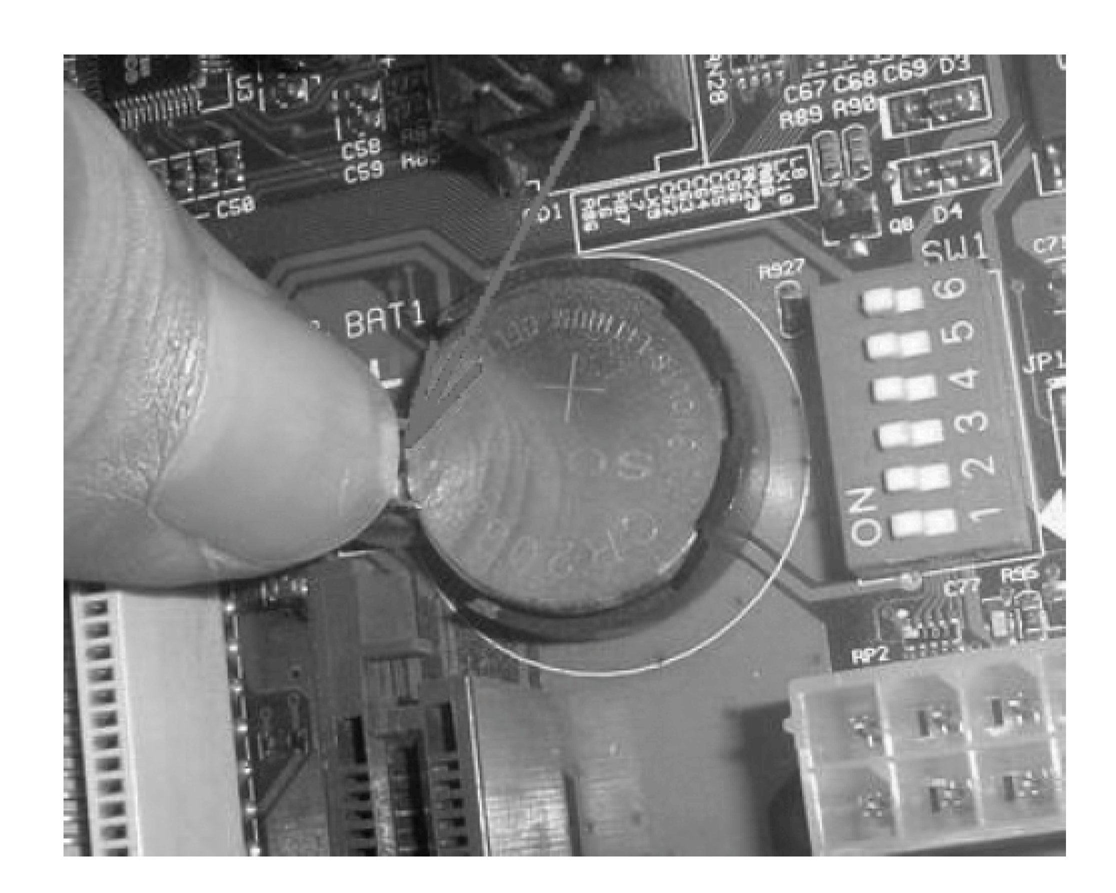


图 2-24 主板电池

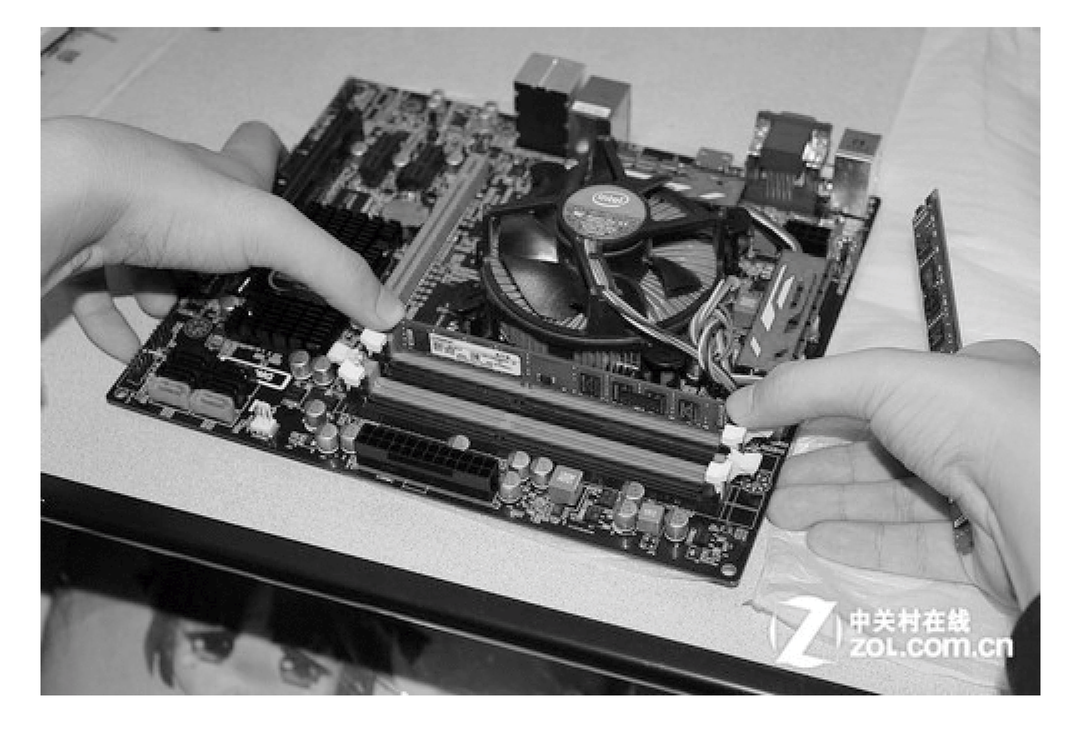


图 2-25 将内存条重新插上

2.4.3 中央处理器常见故障及维护

1. 常见 CPU 故障处理方法

(1) 检查风扇是否运转正常。

由于 CPU 运转时散发很高的热量,需要散热器和散热风扇驱散热量,风扇一旦出现故障,CPU 就会工作不正常甚至被烧毁。

(2) 检查 CPU 是否安装正确。

检查 CPU 安装是否到位,安装 CPU 时要将 CPU 上的小三角对准主板 CPU 插座上的小三角,要和主板 CPU 插座一致才能安上。

(3) 检查 CPU 是否烧毁与压坏。

关机后切断电源,取出 CPU 然后观察 CPU 是否有损毁或针脚是否有压弯的现象。

(4) CPU 本身质量的问题。

2. CPU 超频后出现蓝屏

CPU 超频使用后,在 Windows 操作系统中经常出现蓝屏,无法正常关闭程序,只能重新启动。蓝屏现象一般在 CPU 执行比较繁重的任务时出现,如运行大型的 3D 游戏、处理运算量非常大的图片或影像等。CPU 运行频率过高,导致 CPU 温度急剧上升,从而出现蓝屏,解决此问题步骤如下:

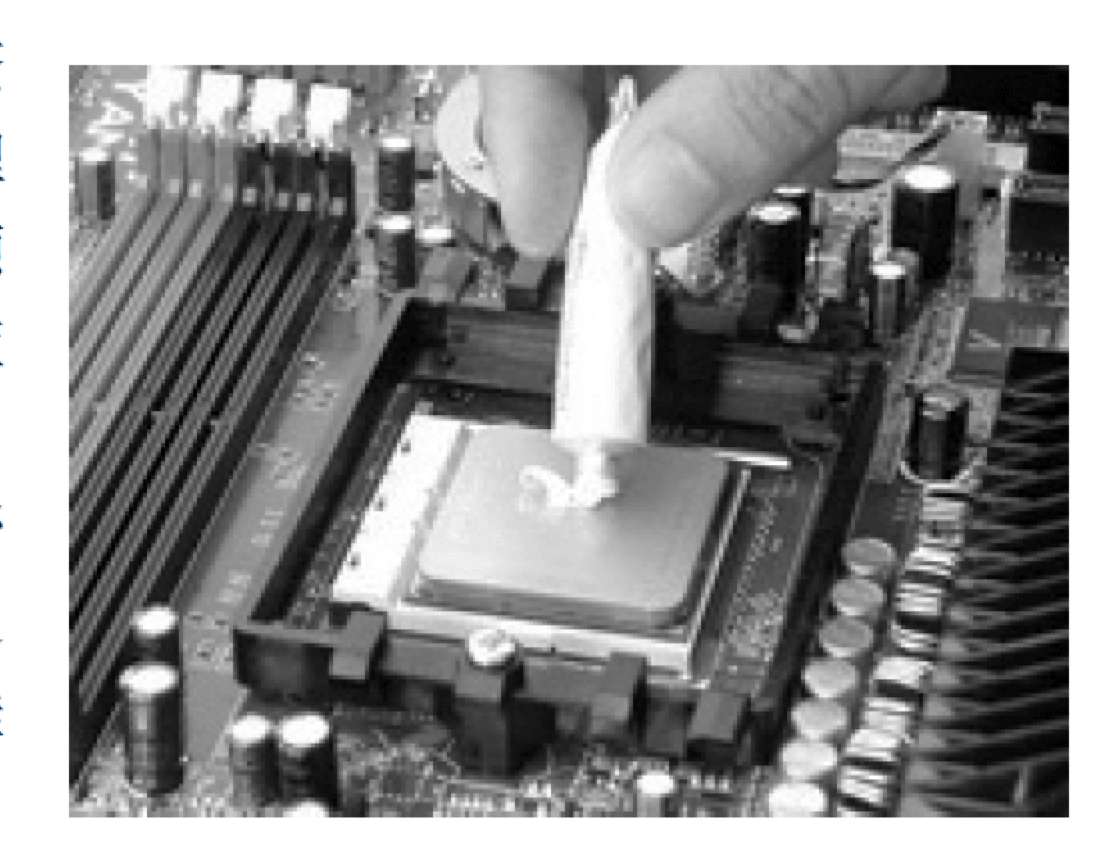


图 2-26 涂抹硅脂

(1) 检查 CPU 表面温度和散热风扇是否正常运转,查看 CPU 和 CPU 风扇是否接触良好,并在两者的接合面上涂抹薄薄的一层硅脂,如图 2-26 所示。

(2) 如果还是不能达到散热要求,则需要更换更大功率的散热风扇。

(3) 如果用以上方法仍然无法排除故障,则建议用户将 CPU 主频恢复至正常工作频率。

3. 计算机不断自动重启

计算机启动后,系统启动一切正常,但是运行一段时间后就自动重启,然后还能正常启动,但是在运行过程中不断重启,解决此问题步骤如下:

(1) 打开机箱侧面板,检查 CPU 风扇,发现 CPU 风扇不转,可能是风扇积尘太多导致。取下风扇,用刷子将风扇上的灰尘刷干净。

(2) 把风扇上的贴纸揭起一半,露出轴承,如果轴承处的润滑油已经干涸,可以使用机油在上下轴承处各滴上一滴,然后用手转动几下,擦去多余的机油并重新粘好贴纸,把风扇重新装回散热器,再重新装到 CPU 上面。

(3) 启动计算机,风扇开始转动,运行一段时间,系统运行正常,表明故障已经排除。

4. 正常操作计算机时突然黑屏

在正常使用计算机时突然出现黑屏,重新启动系统后仍然黑屏,但电源指示灯却一直处于开启状态,解决此问题步骤如下:

(1) 拆下不重要的板卡和设备,例如网卡、声卡等。拆板卡和设备注意,基本要求是保留系统工作的最小配置,以便缩小故障的范围。如果重启计算机后故障一直存在,则更

换显卡，测试其是否恢复到原有状态。

(2) 检查 CPU 上的风扇工作是否正常，将其拆下，把 CPU 取下并重新安装一次，发现系统恢复正常，则说明此故障是由于 CPU 插座松动造成的。将上述部件重新安装好后，即可排除故障。

2.4.4 存储设备常见故障及维护

1. 内存

内存是计算机主要的组成部件，负责运行过程中数据的读取和存储，内存出现故障时，可能会导致计算机无法启动或者死机。

(1) 常见内存故障的排除方法。

常见内存故障，主要有以下两种排除方法：

① 清洁法。内存故障在很多情况下是由于接触不良造成的，由于内存金手指长期暴露在空气中，形成一层氧化物，造成与主板内存槽接触不良，或是有灰尘引起的接触不良。用酒精、橡皮、硬纸片以及专用的清洗液等工具对内存金手指氧化物或内存插槽中的污垢进行清理。

② 替换法。为了辨别和找出故障原因，需要用一条好的内存条连接到出现故障的计算机中，或将故障内存条插到好的计算机中，通过观察来判定内存是否出现问题。

(2) 运行某些软件时出现内存不足的显示。

这种现象多是由于计算机内存容量比较小，而在系统中又对虚拟内存加以限制而造成的，解决此问题步骤如下：

① 在桌面“我的电脑”图标上单击右键，选择【属性】→【高级】→【性能设置】选项，打开“性能选项”对话框，选择“高级”标签，单击“虚拟内存”栏中的【更改】按钮，如图 2-27 所示，将打开“虚拟内存”对话框。

② 在“虚拟内存”对话框中，将虚拟内存指定到可用空间较大的分区盘上，例如 C 盘，定义虚拟内存的大小，如图 2-28 所示。

(3) 系统中显示的内存容量偏低。

在 Windows XP 操作系统的“系统属性”对话框中查看内存容量，发现其显示的数字小于实际容量。造成系统显示的内存容量小于实际容量有以下三种原因：

① 主板上集成了显卡，并与系统共享内存，系统启动时就必须分配给显卡一部分内存作为显存使用。

② 检查 BIOS 设置中的 Memory Hole At 15MB～16MB 选项是否启用，若启用，则在系统启动时会将 15MB 内存划分出来供 ISA 接口设备使用，这样留给 Windows 系统的内存就会减少 15MB，若未安装此类 ISA 设备，将此选项禁用。

③ 查看 autoexec. bat 文件，如果其中设置了启动时将 smartdrv. exe 文件载入内存，则系统会默认分配 1MB 内存当作磁盘缓存。




图 2-27　打开“虚拟内存”

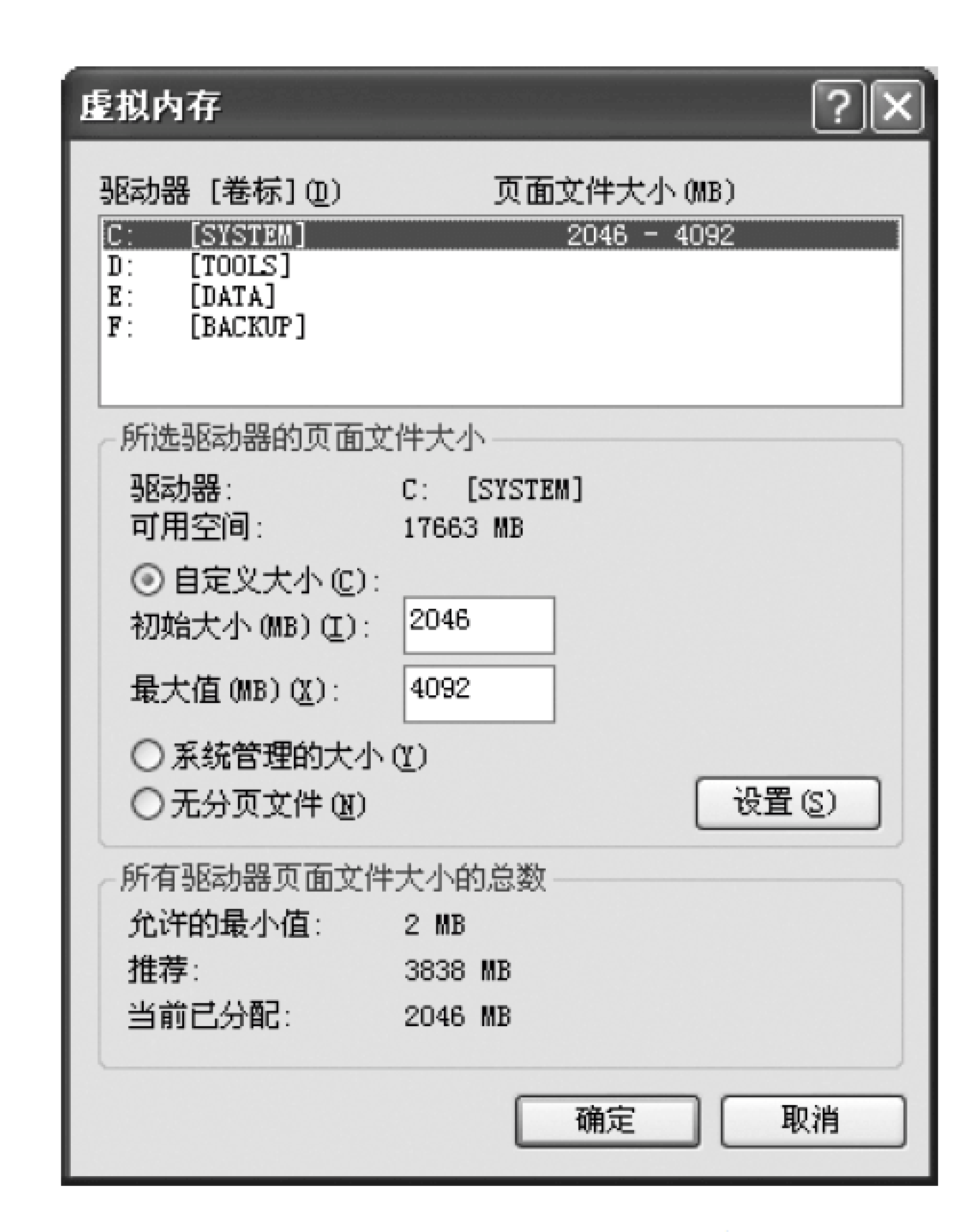


图 2-28　设置“虚拟内存”

（4）内存条过热时系统死机。

在使用计算机的过程中，系统经常出现“内存不可读”的提示错误信息，随后出现一些英文提示并死机。这种问题经常出现，且没有规律，往往天气热的时候出现的几率较大。

因为系统已经提示“内存不可读”，所以先从内存上来寻找排除故障的方法。天气热时该故障出现的几率较大，一般是由于内存条过热而导致系统工作不稳定。

用户可以自己加装机箱风扇，以加强机箱内部的空气流通；还可以通过给内存加装铝制或铜制的散热片来解决问题。

2．硬盘

硬盘是负责存储软件资料的仓库，硬盘的故障如果处理不当往往会导致系统无法启动和数据丢失。

（1）常见硬盘故障。

① 系统找不到盘，一般是由于硬盘数据线和电源线没有接好，硬盘主从跳线设置错误或 BIOS 设置错误等。可以通过重新插接并重设 CMOS 参数，发现故障所在。

② 由于突然断电、病毒破坏、软件使用不当造成硬盘分区损坏时，不能启动硬盘，可以用分区软件重建分区表。

③ 硬盘坏道处理。硬盘一般有两种坏道：一种是逻辑坏道，可以通过软件或者低级格式化修复；另一种是物理坏道，即硬盘磁盘上出现划痕，主要是由于硬盘质量不佳、电源电压不稳、温度不当、人为损坏等造成。

（2）硬盘无法识别。

系统无法识别硬盘是最为常见的硬盘故障之一。通常情况下，很多用户遇到这一故

障，首先想到的是硬盘损坏了，从而不加判断地将硬盘做报废处理。其实，很多情况下，硬盘并没有损坏，稍加处理即可排除此类故障，解决此问题步骤如下：

① 打开机箱，检查硬盘数据线是否插到位，是否安装牢固。最为简单的方法是拔下硬件数据线，除尘后进行重新插拔。

② 如果有双硬盘，检查主从跳线是否设置正确。

③ 在硬盘加电时注意听，注意硬盘盘片是否运转正常以及转动有没有异常。如果出现了不规则的“嘎嘎”或者“当当”声，然后伴随死机，或者根本不运转的，则可确认是硬盘出现了物理故障。

④ 如果出现以上情况，则应该检查硬盘是不是被病毒破坏了分区表和引导区，或是否中了硬盘的逻辑锁。出现这种情况应该用系统盘启动，在 DOS 下运行杀毒软件进行杀毒。如果硬盘分区表和引导区数据有备份，恢复硬盘分区表。

(3) 磁盘分区的盘符混乱交错。

计算机原有一块硬盘，分为 C 和 D 两个分区，后又安装了一块分为三个分区的硬盘，结果原硬盘的 D 区变为 E 区，新硬盘的 C 区变为 D 区、D 区变为 F 区、E 区变为 G 区，而原来安装的 D 区的软件现在都无法正常运行了。

这是操作系统对硬盘的特殊管理方法产生的故障。新旧两块硬盘的 C 区都是主分区，而其他分区是逻辑分区，操作系统会将主盘的主分区识别为 C 区，而将从盘的主分区识别为 D 区，然后再将主盘的各逻辑分区、从盘的各逻辑分区依次识别为 E、F 等分区，解决此问题步骤如下：

① 在 BIOS 设置程序中将第二块硬盘设置为 None。操作系统的“即插即用”功能会在启动时检查出该硬件，并自动依次分配原盘符之后的盘符。

② 在 Windows XP 操作系统中，可以直接在“计算机管理”对话框中展开“计算机管理(本地)”|“存储”|“磁盘管理”对盘符进行修改，如图 2-29 所示。

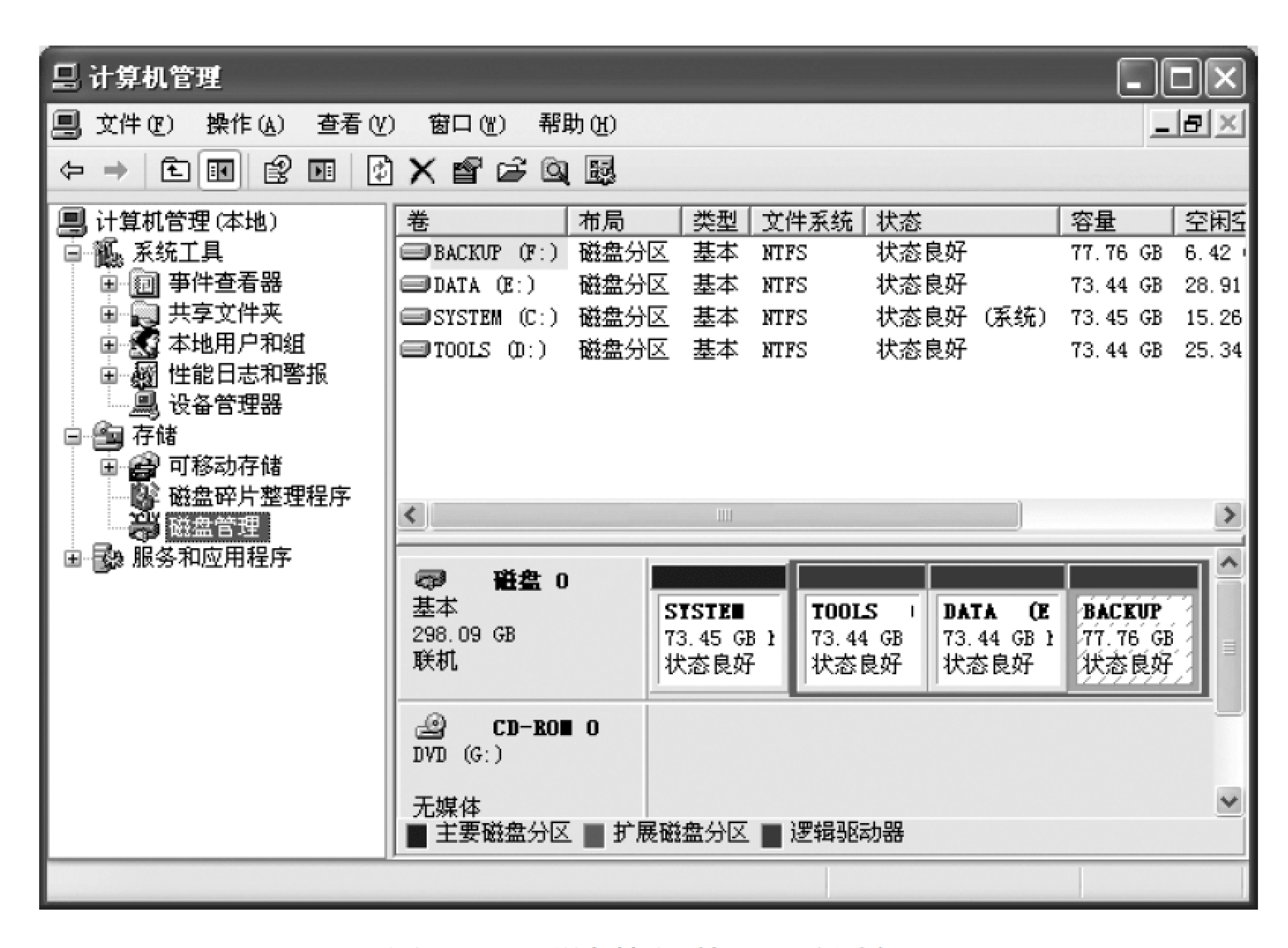


图 2-29 “计算机管理”对话框

(4) 屏幕提示 Hard disk(s) Diagnosis fail。

关闭计算机一段时间后在开机,屏幕上出现错误提示信息:Hard disk(s) Diagnosis fail,硬盘灯一直闪烁,系统却无法正常启动。但隔一段时间后再启动计算机,故障消失。

根据故障现象判断是硬盘出了问题,由于在关机一段时间以后出现此故障,分析可能是硬盘的磁头不能很快归位从而导致系统诊断失败,解决此问题步骤如下:

① 打开机箱,在硬盘的外壳上轻轻敲击。

② 安装好硬盘并重新开机。

③ 如若故障没有排除,则联系产品维修点对硬盘进行维修。

3. 光驱故障与维修

光驱是计算机硬件中使用寿命最短的配件之一。其实很多报废的光驱仍有很大的利用价值,只要略微维修一下就可以了。这往往不需要具有什么高深的无线电专业知识,也不需要使用什么太复杂的维修工具及材料。用户只要细心观察故障现象并参照执行下面的一些排除方法,老光驱就能恢复使用。

(1) 光驱内的光盘打滑。

将光盘放入光驱之后,可以听到激光头移动和搜索的声音,接着听到摩擦声,最后光驱灯常亮不熄灭。造成此故障的原因主要有以下两个方面:

① 光驱长期使用后,由于没有对光驱产生足够的压力,从而导致盘片转动时打滑。

② 由于盗版光盘在制造时偷工减料,使得光盘的厚度比正版的光盘薄些,与光驱产生摩擦。

更换质量好的光盘,如果故障依旧存在可能是光驱老化造成的,只能更换光驱了。

(2) 光驱面板上的【开仓】键无法使用。

光驱使用频繁,有的时候光驱面板上的开仓键会失灵,有时候按下去,光驱托盘却弹不出来,这类是光驱的硬件问题,简单的办法是通过“软”控制解决,步骤如下所示:

① 通过软件来弹出或者关闭光驱托盘,像超级解霸之类的播放工具都提供【弹出】和【关闭】按钮,可以用来控制光驱。

② 如果软件也无法控制,可以用一根曲别针插进光驱前面板的紧急出盒孔,这样托盘就会自动弹出。

(3) 放入光盘后马上被弹出。

DVD 光驱开机加电后,指示灯闪烁 10 秒后停止;按【出仓】按钮光驱托盘可以打开,但放入光盘后又马上被弹出。

根据故障现象分析,该故障可能是激光头与电路板之间的连接线故障、主轴电机与其驱动电路的连线故障或光驱的电路板故障引起的。打开光驱的外壳,检查激光头与电路板之间的连接线,如果发现连接线中有断线,更换此连接线之后,故障即可排除。

2.4.5 电源常见故障及维护

计算机的电源是主板、CPU、硬盘、内存等其他部件的动力源泉,没有电源计算机也就无法工作。主机开关电源的稳定性高低,输出电压的准确与否,输出电流的质量高低,

都关系着计算机是否能够正常工作，能否长时间运行。

1. 电源的保养

电源将高压的220V交流电转变成+12V、+5V等的低压直流电，再供给计算机内的各个部件使用。电源中处理高压的部分，包括整流器和高压开关晶体管等，如果受到高压的冲击，损伤比较大，寿命会缩短，因此要选用质量好的电源。用户能做的就是保持电源工作时的良好环境，炽热是电源的大敌，会损坏内部的所有零件，无论如何一定要避免，否则电源的寿命会大大缩短。

保持电源工作时的良好环境应达到以下两点要求：

① 出风口要留有足够的空间。使电源保持低温最简单的方法是将计算机和墙壁之间留有足够的空间。

② 保持电源风扇的清洁。与CPU的散热风扇一样，电源风扇也应该注意清洁。但清洁电源风扇是要拆开电源变压器，操作时应该十分小心，尽量不要接触风扇以外的其他部件，以免发生意外。

2. 计算机升级之后系统无法正常启动

电脑升级后，系统经常无法正常启动，或者在工作时意外重启。

根据故障现象分析，可能是原来使用的电源无法达到新系统的功率要求而造成的。更换为高质量电源后，故障消失。

3. 计算机每次开机时，只要接通电源，不用按开机按钮就会自动启动

此故障可能是由于主板BIOS设置不当或计算机电源故障引起的，解决此问题步骤如下：

（1）开机按Del键进入BIOS设置程序，进入Integrate Peripherals设置项，选择Power On After PW-Fail选项，将参数On改为Off即可。

（2）若故障依旧，可能是电源故障，需要更换电源。

4. 休眠与唤醒功能不正常

计算机的休眠与唤醒功能不正常，不能进入休眠状态。此故障可能是电源引起的，另外旧主板也不能很好地支持休眠功能，解决此问题步骤如下：

第1步：更换一个功率大一点的电源试一下。

第2步：如果是旧主板，则要更换主板或者关闭休眠功能。

（1）打开“控制面板”窗口，如图2-30所



图2-30 “控制面板”窗口

示，双击“电源选项”电源选项图标，打开“电源管理 属性”对话框。

（2）在“电源管理 属性”对话框中选择“电源使用方案”标签，将“关闭显示器”、“关闭硬盘”、“关闭待机”三个选项均设为“从不”，如图 2-31 所示。

（3）在“电源管理 属性”对话框中选择“休眠”标签，在“休眠”选项区域中勾选“启动休眠”复选框即可，如图 2-32 所示。



图 2-31 “电源管理 属性”对话框



图 2-32 “休眠”标签界面

2.4.6 显示系统常见故障及维护

显卡、显示器是计算机的主要展示窗口，如果它们出了故障，计算机也就无法操作，因此平时一定要做好保养和维护工作。

1. CRT 显示器屏幕边缘闪烁

屏幕边缘闪烁通常是由于显示器行电路部分元件虚焊或电源处的＋300V 滤波电容容量减小所致；有些机型的供电部分的某一元件虚焊也会造成此故障；另外，某些显示器的分辨率和刷新率设置得偏高或偏低也可能造成此类故障。解决此问题步骤如下：

（1）检查显示器附近是否有带磁物品，如有的话，将其清除。

（2）检测显卡的驱动程序是否存在 Bug，尝试更新驱动程序。

（3）把分辨率和刷新率设置成中间值进行测试。

（4）检查高压包产生的加速极电压和高压是否正常，有时这两个电压异常也会导致此类故障。

2. CRT 显示器屏幕总是闪烁

计算机工作时，CRT 显示器的屏幕有明显的闪烁现象，用户看得时间久了眼睛会非常疲劳。屏幕闪烁一般是屏幕刷新率过低所致，将屏幕刷新率在所允许的范围内调高即

可解决此问题。解决此问题步骤如下：

(1) 在桌面的空白位置右击，在弹出的快捷菜单中选中“属性”命令，将打开“显示 属性”对话框。

(2) 选择“设置”标签，单击【高级】按钮，在打开的对话框中选择“监视器”标签。

(3) 在“屏幕刷新频率”下拉框中选择一个合适的刷新率。一般情况下，75Hz 基本可以接受，85Hz 以上就没有闪烁的感觉了，如图 2-33 所示。



图 2-33 选择合适的刷新频率

3. 使用集成显卡提示缓存不足

计算机使用的是集成显卡，在运行过程中经常出现刷新不流畅的现象，有时系统还会提示缓存不足。解决此问题步骤如下：

(1) 重新启动，按 Del 键进入 BIOS 设置程序。

(2) 将 Integrated Peripherals 中的 VGA Shared Memory Size 选项的值都设置成 16MB 以上。

(3) 按 F10 键保存设置，退出 BIOS 设置程序后，重新启动计算机更改显存即可。

4. 玩 3D 游戏时出现花屏或死机

大型 3D 游戏对硬件要求非常高，任何一个硬件达不到要求都会使游戏卡住，甚至出现花屏或死机现象。尽管游戏画面主要是靠显卡来渲染，但不一定是显卡质量不好造成的花屏故障，还应该具体问题具体分析。解决此类问题步骤如下：

(1) 检查主板或电源。如果是主板无法为显卡提供足够大的电源功率，则可以进入 BIOS 设置界面，适当提高主板的显卡供电电压。

(2) 如果是电源引起的，则更换一个大功率的电源。

(3) 到网上查找相应型号的显卡驱动程序，及时将本地系统的显卡程序升级到最新版本，以便显卡能充分发挥其性能。

(4) 检查“Direct3D 加速”是否已经开启。

在 Windows 桌面选中“开始”→“运行”命令，打开“运行”对话框，输入 dxdiag，如图 2-34 所示，单击【确定】按钮，打开“DirectX 诊断工具”对话框，确保 Direct3D 和“DirectDraw 加速”选项启动，如图 2-35 所示。



图 2-34 “运行”对话框

5. LCD 液晶显示器的保养

(1) 温度。

LCD 液晶显示器应在 5℃—40℃工作。



图 2-35　打开“DirectX 诊断工具”对话框

（2）湿度。

LCD 液晶显示器适合的湿度为 0℃～40℃。

（3）清洗。

清洗要轻柔，可用柔软的纸巾轻擦，或用软布蘸少许清水但不要有水滴轻轻擦拭 LCD。

2.4.7　打印机、扫描仪故障及维护

1. 打印机

打印机是使用最频繁的办公设备，在使用打印机的过程中，可能会遇到各种各样的打印故障，如打印机不能进纸、打印文件时卡纸、打印效果不佳、系统无法添加打印机、打印乱码等。下面介绍打印机常见故障的诊断与排除。

（1）打印字符错位。

打印字符错位可能是在运输或搬移打印机的过程中打印头错位所引起的，另外打印头在使用过程中撞车也可能引起打印字符错位。解决此问题步骤如下：

① 使用打印机附带的“打印校准程序”来校准打印头。

② 如果没有打印校准程序，在打印时设置打印机为单向打印也可解决问题，但是会影响打印速度。

（2）不能正常连接打印机。

如果出现不能正常连接打印机，可以通过以下步骤加以解决：

① 检查打印机是否已经开启。

② 检查确认打印机已经连接到正确的端口上，确认打印机电缆线已经连好。

③ 如果还不行，进入 BIOS，检查并行通信端口有没有被使用。

(3) 无法在网络中共享打印机。

办公室新添了一批计算机，在共享网络打印机的设置中遇到了问题，终端无法在网络上找到共享的打印机。

根据故障现象分析，打印机已设置了共享，网络也没有问题，仔细查看系统，发现 Windows 防火墙开启，限制了打印机的共享，解决此问题的步骤如下：

① 在桌面选中“开始”→“控制面板”命令，打开“控制面板”对话框，在其中双击“防火墙”图标，如图 2-36 所示。

② 在打开的“Windows 防火墙”对话框中选择“常规”标签，选中“关闭(不推荐)”选项，如图 2-37 所示，然后单击【确定】按钮，关闭该对话框，即可解决问题。



图 2-36 “控制面板”窗口

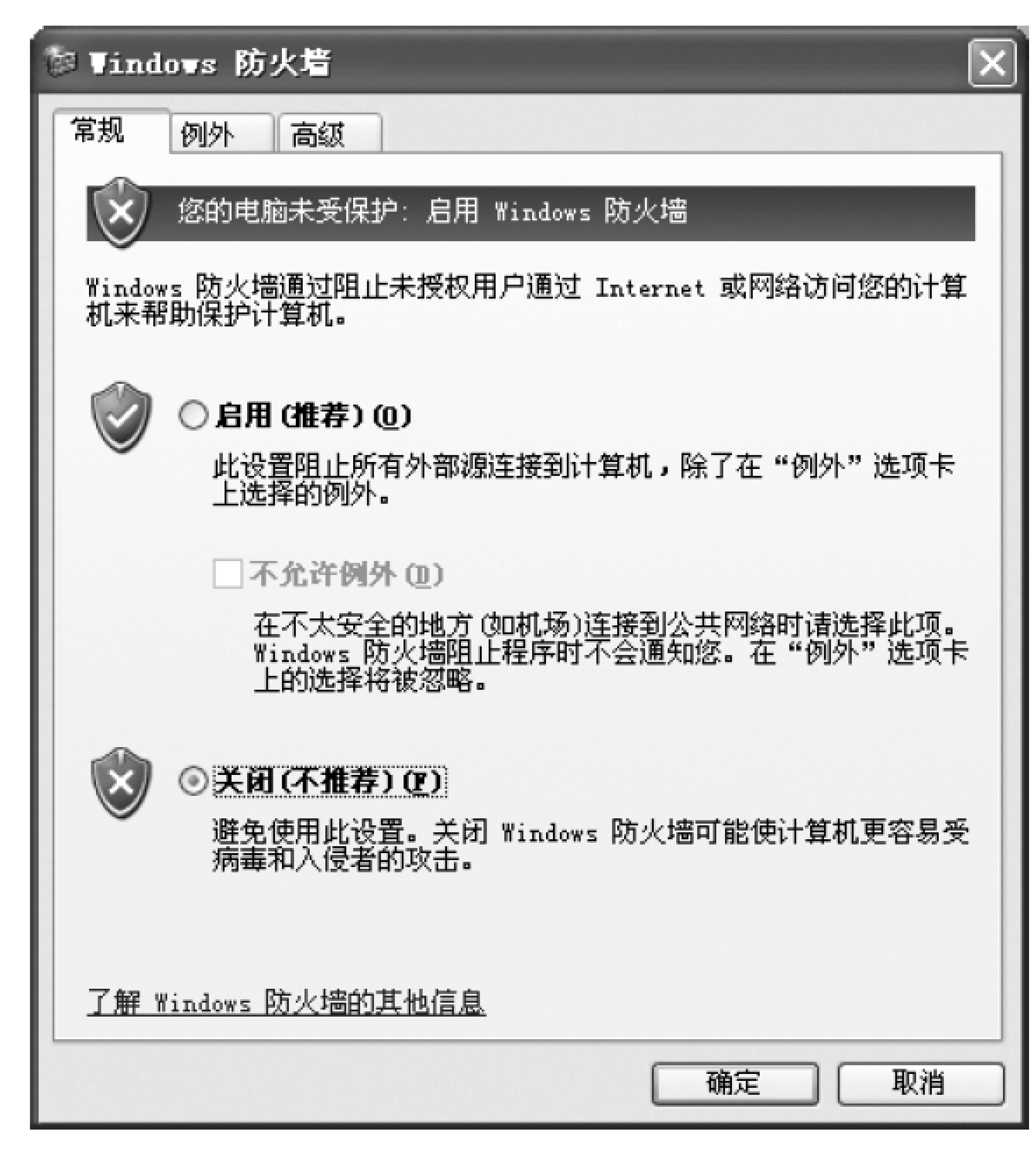


图 2-37 “Windows 防火墙”对话框

2. 扫描仪

扫描仪是一种广泛应用于现代办公的输入设备，它作为光电、机械一体化的高科技产品，一旦出现故障就会令用户束手无策，显然有些故障需要找专业人员进行维修，但是也有许多故障是用户可以自行排除的。下面介绍扫描仪的常见故障及排除方法。

(1) 无法连接扫描仪。

使用扫描仪进行扫描时，提示无法连接扫描仪，此故障应该是计算机未找到扫描仪所致，解决此问题步骤如下：

① 检查扫描仪的电源和数据线是否连接好。

② 进入“设备管理器”，检查是否显示该扫描仪设备。

③ 检查扫描仪的指示灯是否正常，如果指示灯闪烁，说明该扫描仪状态不正常，重新安装扫描仪驱动程序。

④ 查看该设备的 IRQ 或 I/O 地址是否冲突，进行相应的修改。

（2）扫描图像时系统提示内存不足。

使用扫描仪对图像进行扫描时，系统总是提示内存不足，防止出现提示框的方法如下：

① 右击桌面上“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，弹出“系统属性”对话框，如图 2-38 所示。



图 2-38 “系统属性”对话框

② 在“系统属性”对话框中选择“高级”标签，单击“性能”框中【设置】按钮，打开“性能选项”对话框，如图 2-39 所示。

③ 在“性能选项”对话框选择“高级”标签，在“虚拟内存”框中单击【更改】按钮，如图 2-40 所示，打开“虚拟内存”对话框。



图 2-39 “性能选项”对话框

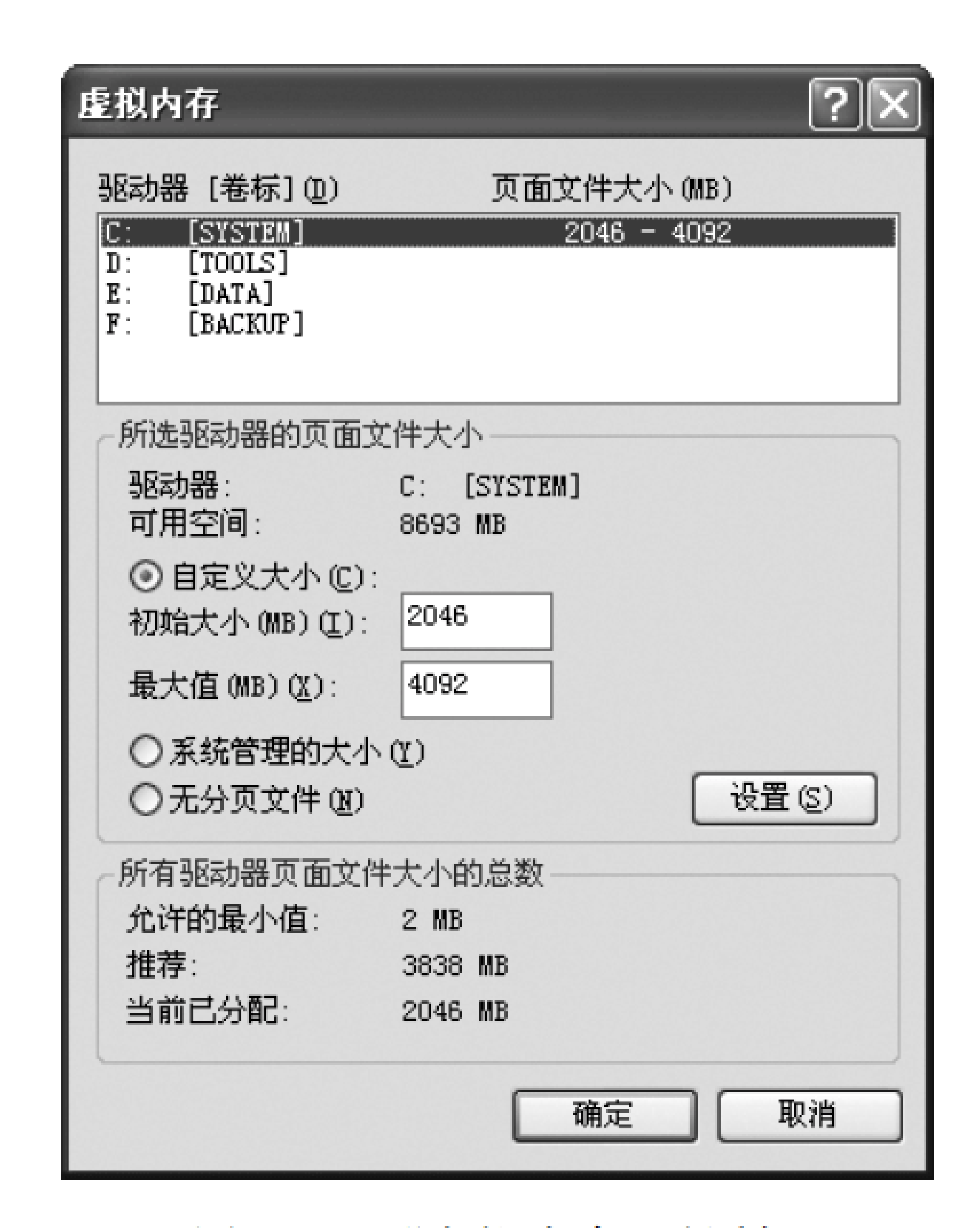


图 2-40 “虚拟内存”对话框

④ 在“虚拟内存”对话框，将虚拟内存的容量调大，单击【确定】按钮即可，如图 2-40 所示。

2.4.8 网络设备常见故障及维护

1. 网卡设备

计算机要接入网络，无论是单位的局域网，还是资源丰富的互联网，网卡都是必不可少的设备之一。对于普通用户而言，上网过程中遇到的网络故障有相当一部分是与网卡相关的。下面介绍与网卡设备相关的几种故障及排除方法。

（1）网卡设备无法正常识别。

在计算机使用过程中无法连接到网络，打开设备管理器，发现在网络适配器选项下有一个黄色的惊叹号或黄色的问号，或者是红色的叉号。遇到这种情况，大多是网卡驱动没有正确安装或者是网卡被禁用造成的，解决此问题步骤如下：

① 在 Windows 桌面选中“开始”→“运行”命令，打开“运行”对话框，输入“devmgmt.msc”命令，单击【确定】按钮后，打开“设备管理器”对话框，如图 2-41 所示。

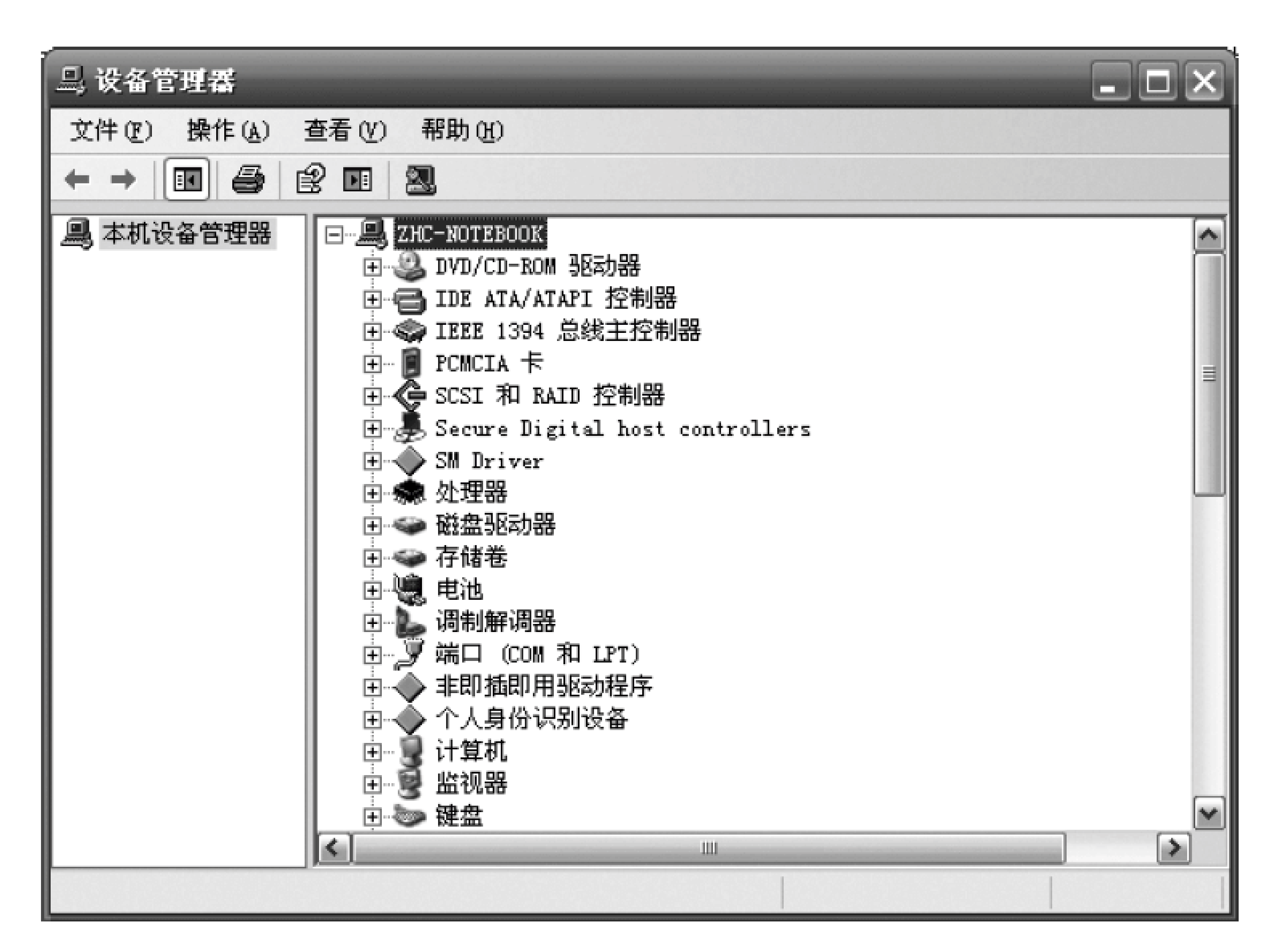


图 2-41 “设备管理器”对话框

② 如果在网卡设备上是一个红的叉号，可以在网卡设备上右击，选择“启用”命令即可。

③ 如果是黄色的问号或者是惊叹号，则是网卡驱动没有正确安装造成的。在网卡设备上右击，选择“卸载”或“删除”命令，将故障网卡卸载。

④ “设备管理器”对话框菜单栏选择“操作”→“扫描检测硬件改动”菜单命令，计算机会重新扫描检测网卡设备，发现新硬件后会自动安装驱动，至此故障即可排除。

⑤ 如果故障依然存在，可能是用户的网卡比较特殊，计算机自带的驱动无法正确识别并安装驱动。这时，可以重复“步骤 3”，将故障网卡卸载，然后插入网卡自带的驱动程序光盘，手动安装驱动，驱动安装完毕重启计算机，网卡即可正确识别。

（2）安装网卡后启动速度变慢。

局域网方便了工作和用户之间的沟通互联。但很多用户发现自己接入局域网之后，

系统启动速度比联网前慢了很多，可找不到原因。

这种故障多发生在采用 DHCP 动态分配 IP 地址的局域网中，客户端计算机采用自动获取 IP 地址的方式。系统启动时除了需要检测网络连接外，还要自动检查网络中的 DHCP 服务器，从而增加了系统的启动时间，用户可以通过以下方法改善速度慢的状况。

① 右击桌面“网上邻居”图标，选择“属性”命令，打开“网络连接”对话框。

② 在“网络连接”对话框右击“本地连接”，选择“属性”命令，打开“本地连接属性”对话框，选择“常规”标签，在“此连接使用下列项目”框中选择勾选“Internet 协议(TCP/IP)”选项，如图 2-42 所示，单击【属性】按钮，打开“Internet 协议(TCP/IP)属性”对话框，如图 2-43 所示。



图 2-42 “本地连接 属性”对话框

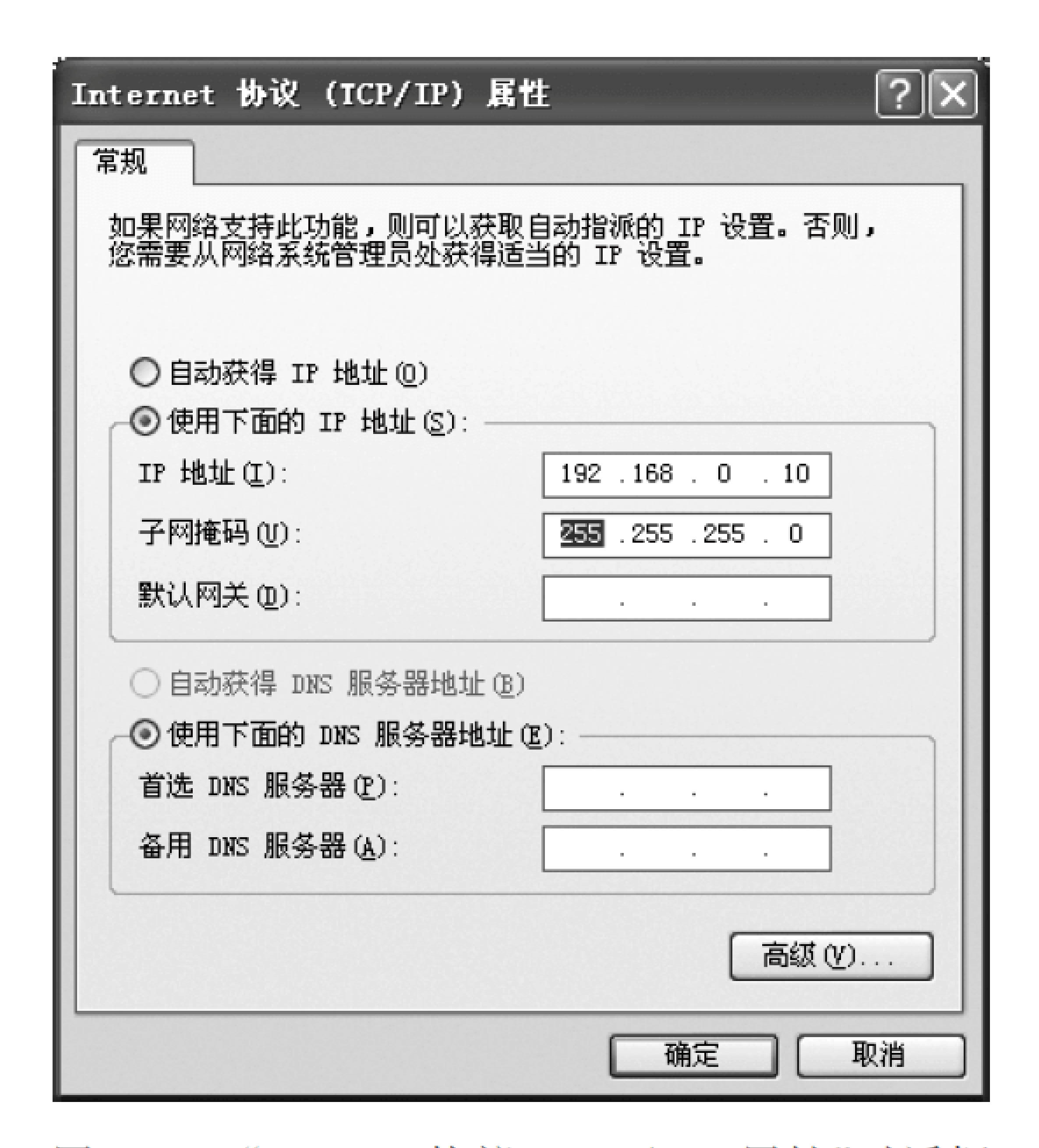


图 2-43 “Internet 协议(TCP/IP) 属性”对话框

③ 在“Internet 协议(TCP/IP)属性”对话框中，将“自动获得 IP 地址”选项改为“使用下面的 IP 地址”，然后在 IP 地址、子网掩码、默认网关、DNS 等文本框中输入网管分配过来的 IP 地址和相关信息，如图 2-43 所示。

(3) 重启计算机之后找不到网卡。

一台计算机重启后找不到网卡，在设备管理器中反复刷新或重启计算机也无法解决问题。此故障可能是网卡接触不良或灰尘太多造成的。解决此问题步骤如下：

① 打开主机箱，卸下网卡，用橡皮擦拭网卡的金手指。

② 为网卡槽清理灰尘，再安装上网卡。

③ 如果故障依旧，将其换到其他插槽内重新开机即可。

2. 路由器

路由器(router)是连接因特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径，按前后顺序发送信号。路由器是互联网络的枢纽，被称为

“交通警察”。路由器广泛应用于各行各业,各种不同档次的路由器产品已成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的关键设备。

下面介绍路由器的常见故障及排除方法。

(1) 忘了路由器用户名和密码。

故障:一台无线宽带路由器,连接了台式机和笔记本电脑,几天后突然发现无法正常上网。经过仔细检查,发现网络连接没有问题,ADSL也能正常连接。在浏览器中的地址栏中输入“192.168.0.1”,打开路由器配置界面,此时系统提示输入用户名和密码,可由于时间长了,自己忘记了管理员密码。

排除方法:按路由器的复位按钮,将路由器复位后,故障就会消失。

(2) 路由器升级后无法联网。

故障:一台无线路由器(TP-Link TL-WR541G)固件版本较低,只支持加密功能较弱的WEP协议。为了保证通信安全,将无线路由器固件升级为最新版本,但升级后发现无法连接到网络。

排除方法:查看无线路由器指示灯,一切正常,说明固件升级成功,无线路由器处于正常状态。仔细分析,很可能是无线路由器升级后,其参数被初始化为出厂设置造成的。

在客户机中将“无线连接”的SSID参数更改为无线路由器的初始化值tp-link,然后禁用WEP加密功能,故障消失。

(3) 多台计算机连接路由器不可用。

故障:多台计算机连接一个路由器,只有一台计算机可正常上网,其余计算机只能登录QQ等软件,不能上网。

排除方法:要解决这个问题,建议在路由器和计算机网卡上手动设置DNS服务器地址(ISP提供的DNS地址),具体步骤如下:

① 打开路由器设置界面,选择“网络参数”中的“WAN口参数”字段,然后在下面手动设置DNS服务器地址。

② 在“DHCP服务”设置项中,手动设置DNS服务器和备用的DNS服务器地址,该地址需要从ISP服务商那里获取。

2.5 案例讨论

2007年5月16日下午5时,从事金融行业的蒋先生下班回到家中时,发现他的个人计算机因楼上房子漏水导致电脑进水损坏,而且计算机硬盘中存有他大量的私人用户信息和机密文件。在送至计算机维修点拆开主机箱查看后,硬盘、主板等全部进水,维修人员建议放弃计算机。

几天后,蒋先生与房主达成赔偿协议,获得赔偿后的蒋先生考虑到已损坏计算机已不能开机,也就没有在意对已损坏计算机的处理,而以低价卖给了计算机维修部。就在事情过去一个月之后,令蒋先生气愤的事情发生了。

首先是蒋先生的各种用户名密码被莫名地修改,而后蒋先生的银行账户也出现了异常,更有甚者,有人打电话来让蒋先生赎回自己的私人用户信息和机密文件。迫于无奈的

蒋先生只好选择了报警。

经警方调查,被蒋先生卖给维修部的进水计算机又被维修部转卖给了他人,经多方转手后,硬盘最终落到犯罪分子李某手里。李某通过硬盘数据恢复技术获取了蒋先生的用户信息和机密文件,李某遂向蒋先生实施敲诈。直接造成蒋先生经济损失 1 万余元,并对其私人信息的安全性造成严重影响。

通过阅读案例,硬件安全的影响可大可小,不容忽视。作为一名计算机使用者,你认为应该怎么保护计算机硬件安全?应该注意什么问题?应该如何维护硬件与基础设施?

归纳总结

1. 归纳总结保护计算机硬件和基础设施的安全措施。
2. 根据本章内容,总结一下有哪些常见硬件故障,应如何维护。
3. 总结自己所在学校或单位的机房目前都有哪些安全防护措施,分析存在哪些安全隐患,提出改进措施。

思考与实践

思考题

1. 什么是硬件和基础设施安全?它包括哪些部分?
2. 硬件和基础设施主要面对哪些威胁?又该怎样防护?
3. 硬件防复制有哪些方法?除此以外,你还知道哪些?并说明它们的局限性。
4. 为什么要保证计算机机房及环境安全?
5. 列举一些常用的计算机硬件检测工具,它们对计算机硬件安全有什么意义?

实践题

1. 上网搜索近几年由于计算机硬件安全问题所导致的重大事故。
2. 假如现在你所在的学校要建一个大型计算机机房,请给出几点具体建议。
3. 使用硬件大师对自己的计算机硬件进行检测,并形成相关说明性文档。
4. 举例说明你在计算机的使用过程中所遇到的故障及解决办法。



第3章 密码技术

学习目标

通过本章的学习，能够——

- 了解密码与密码学的概念；
- 了解现代密码技术的发展和应用；
- 知道密码技术的典型加密算法；
- 知道密码技术的应用；
- 掌握 Office 文件加密与解密的方法。

引导案例

公元前 405 年，雅典和斯巴达之间的伯罗奔尼撒战争已进入尾声。斯巴达军队逐渐占据了优势地位，准备对雅典发动最后一击。这时，原来站在斯巴达一边的波斯帝国突然改变态度，停止了对斯巴达的援助，意图是使雅典和斯巴达在持续的战争中两败俱伤，以便从中渔利。在这种情况下，斯巴达急需摸清波斯帝国的具体行动计划，以便采取新的战略方针。

正在这时，斯巴达军队捕获了一名从波斯帝国回雅典送信的雅典信使。斯巴达士兵仔细搜查这名信使，可搜查了好大一阵，除了从他身上搜出一条布满杂乱无章的希腊字母的普通腰带外，别无他获。情报究竟藏在什么地方呢？斯巴达军队统帅莱桑德把注意力集中到了那条腰带上，情报一定就在那些杂乱的字母之中。他反复琢磨研究这些天书似的文字，把腰带上的字母用各种方法重新排列组合，怎么也解不出来。最后，莱桑德失去了信心，他一边摆弄着那条腰带，一边思考着弄到情报的其他途径。当他无意中把腰带呈螺旋形缠绕在手中的剑鞘上时，奇迹出现了。原来腰带上那些杂乱无章的字母，竟组成了一段文字。这便是雅典间谍送回的一份情报，它告诉雅典，波斯军队准备在斯巴达军队发起最后攻击时，突然对斯巴达军队进行袭击。斯巴达军队根据这份情报马上改变了作战计划，先以迅雷不及掩耳之势攻击毫无防备的波斯军队，并一举将它击溃，解除了后顾之忧，随后，斯巴达军队回师征伐雅典，终于取得了战争的最后胜利。

二战期间，纳粹特工在探测盟军机密军事情报后，将这些情报传递给他们的负责人，

从而决定作战方针。一次,盟军的检查员截获了一张设计图纸。这张设计草图上是3位年轻的模特,她们穿着时尚的服装。

表面上看起来,设计草图很寻常,然而这张看似"清白"的图纸没能瞒过英国反间谍专家们的眼睛。英国安全局的官员们识破了纳粹特工的诡计,命令密码破译员和检查员迅速破译这些密码。

"大批敌方援军随时可能到来。"最终从这张设计图纸上密码破译员们读出了这样的信息。

原来纳粹特工利用莫尔斯电码的点和长横等符号作为密码,把这些密码做成装饰图案,藏在图上诸如模特的长裙、外套和帽子等图案中。

可见掌握密码技术有着至关重要的作用。

3.1 密码技术概述

随着计算机通信被广泛地应用于商业、金融、政府及军事部门,如何防止日益严重的计算机犯罪,防止信息在通信过程中被非法泄露、删除和修改,已成为全社会关心的问题。密码技术作为信息加密、鉴别和签名的手段,已经成为数学家和计算机学家的主要研究课题。同时密码学也促进了计算机科学,特别是计算机与网络安全所使用的技术,如访问控制与信息的机密性。密码技术已被应用在日常生活,包括自动柜员机的芯片卡、计算机使用者存取密码、电子商务等,密码技术的发展已与人们的日常生活息息相关。

本节主要介绍密码与密码学的基本概念,密码技术的产生与发展历程,密码体制的分类和密码协议。

3.1.1 密码与密码学

1. 密码的基本概念

(1) 密码。

密码是按特定法则编成,用于对通信双方的信息进行明密变换的符号。换而言之,密码是隐蔽了真实内容的符号序列。就是把用公开的、标准的信息编码表示的信息通过一种变换手段,将其变为除通信双方以外其他人所不能读懂的信息编码,这种独特的信息编码就是密码。

密码的基础解释为,主要限定于个别人明白(如一则电文)的符号系统。如密码电报、密码式打字机。作为技术而言,密码是一种用来混淆的技术,它希望将正常的(可识别的)信息转变为无法识别的信息。当然,对相关人来说,这种无法识别的信息是可以再加工并恢复的。

密码在中文里是"口令"(password)的通称。登录网站、电子邮箱和银行取款时输入的"密码"严格来讲应该仅被称作"口令",它不是本来意义上的"加密代码",可以称为秘密的号码。

（2）明文与密文。

明文是原始信息，即信息的原始形式。密文是明文经加密变换后的结果，即信息被加密处理后的形式。

（3）加密与加密方式。

加密是指将原始正常的信息（明文）使用某种规则（加密算法）变换为不被外人理解的非正常信息（密文）的过程，加密是防止有价值的信息被拦截和窃取。

传统加密方式主要采用按字符逐位加密（称为流密码）与按字符分组加密（称为分组密码）。

现代加密方式主要采用按比特加密，每次只加密一个比特（称为序列密码）与按比特序列分组加密，每次处理一个比特分组（称为分组密码）。

（4）加密算法。

进行明密变换的法则，即加密时使用的变换规则称为加密算法，复杂的规则可以用函数来表示并进行计算。

加密算法的基本类型可以分为以下四种：

① 换位——按照规定的图形和线路，改变明文字母或数码等的位置成为密文；

② 代替——用一个或多个代替表将明文字母或数码等代替为密文；

③ 密本——用预先编定的字母或数字密码组，代替一定的词组单词等，变明文为密文；

④ 加乱——用有限元素组成的一串序列作为乱数，按规定的算法，同明文序列相结合变成密文。

以上四种加密算法，既可以单独使用，也可以混合使用，以编制出各种复杂度很高的实用密码。

（5）解密与解密算法。

加密的逆过程称为解密，其目的是将密文破译为明文。解密是由某种解密算法实现的。解密算法是将密文恢复为明文的规则或变换函数。

（6）密钥。

为了有效控制加密和解密算法的实现，在其处理过程中要有通信双方掌握的专门信息参与，这种专门信息称为密钥，是函数运算中使用的参数。

2. 密码学

随着密码被广泛用于战争，交战双方为了保护自己的通信安全，窃取对方的情报，研究了各种方法，逐渐形成了密码学。它以研究秘密通信为目的，即对所要传送的信息采取一种秘密保护，以防止第三者对信息的窃取。密码学主要包含两部分内容：一是为保护自己的通信安全进行加密算法的设计和研究；二是为窃取对方情报而进行密码分析，即密码破译技术。

密码学作为一门学科，属于数学的一个分支，是密码编码学和密码分析学的统称。

密码编码学（简称编码学）主要研究密码变化的客观规律，设计难以被敌方或对手攻破，只能被己方知道的以不同加密算法构成的安全密码体制，即怎样编码，采用什么样的

密码体制以保证信息被安全地加密，是研究信息保密的科学和技术。

密码分析学(简称破译学)主要研究在未知密钥的情况下如何从密文推演出明文或密钥，破译敌方或对手已有的密码体制，应用于破译密码以获取通信情报，是研究破译密文的科学和技术。密码分析人员一般需要凭借经验，通过统计分析等方法，而不是通过逻辑导出。密码分析学通常采用两种方法：演绎法和归纳法。近年来，使用计算机进行密码分析从很大程度上提高了破译的能力。

3. 密码体制

密码体制也称密码系统，是指能完整地解决信息通信安全中的机密性、数据完整性、认证、身份识别、可控性及不可抵赖性等问题一个或几个的系统。一个密码体制的正确描述，需要用数学方法清楚地描述其中的各种对象、参数、解决问题所使用的算法等。

任何一种密码体制都包含 5 个要素：明文、密文、密钥、加密算法和解密算法。

(1) 明文：是加密输入的原始信息，通常用 m 或 p 表示。所有可能明文的有限集称为明文空间，通常用 M 或 P 来表示。

(2) 密文：是加密处理后输出的信息，通常用 c 表示。所有可能密文的有限集称为密文空间，通常用 C 来表示。

(3) 密钥：是参与密码变换的参数，通常用 k 表示。一切可能的密钥构成的有限集称为密钥空间，通常用 K 表示。

(4) 加密算法：是将明文变换为密文的变换函数，相应的变换过程称为加密，即编码的过程，通常用 E 表示，即 $c=E(K_E,p)$。

(5) 解密算法：是将密文恢复为明文的变换函数，相应的变换过程称为解密，即解码的过程，通常用 D 表示，即 $p=D(K_D,c)$。

对于有实用意义的密码体制而言，总是要求它满足：$p=D(K_D,E(K_E,p))$函数，即用加密算法得到的密文总是能用一定的解密算法恢复出原始的明文来。而密文消息的获取同时依赖于初始明文和密钥的值，如图 3-1 所示。

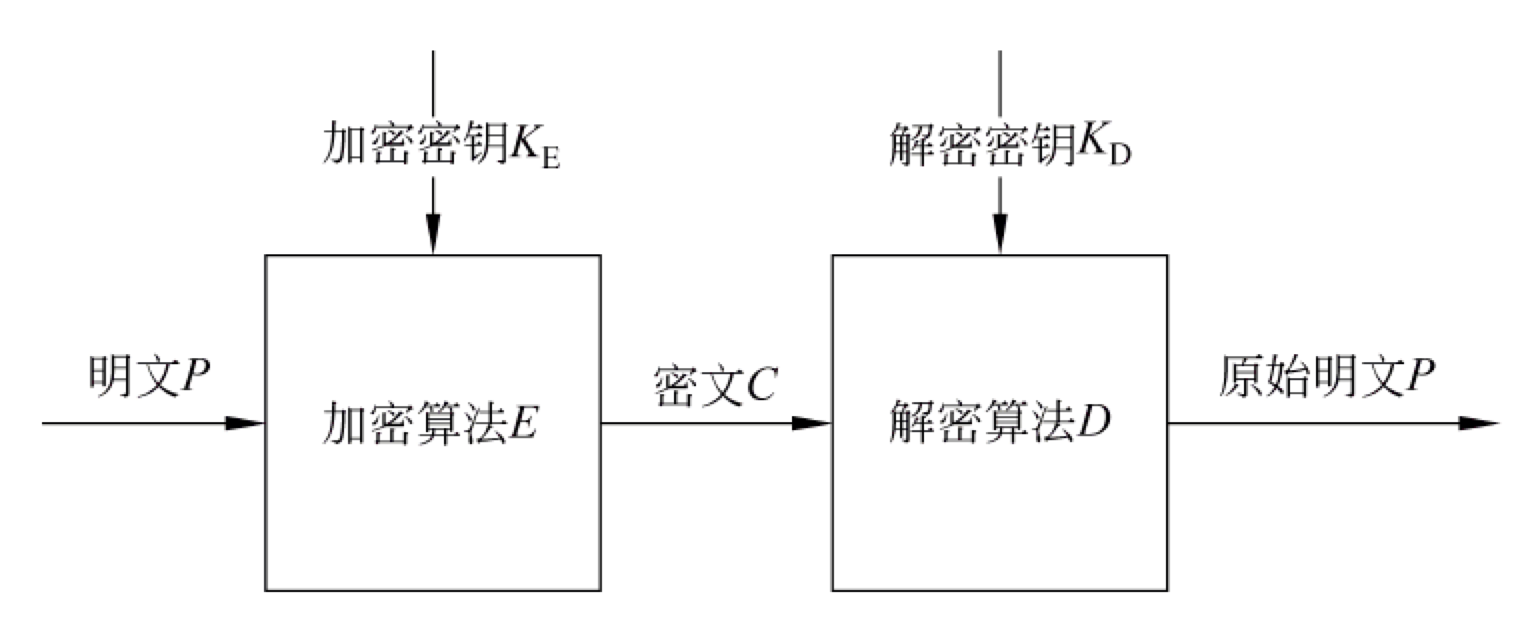


图 3-1　秘密通信过程

秘密通信的过程用文字可以表述为：若发送者要传送的明文 p，在传送前，利用密钥 K 将 p 经加密算法变换为密文 c 由通信通道发给接收者，接收者根据密钥 K 利用解密算法变换将密文 c 变为明文 p。

从以上过程可以看出，一个密码体制的安全性依赖于密钥 K 的个数和加密算法的复杂程度。密钥太少，敌方可以根据其截获的密文用不同的 K 逐个试译即可得到明文。也

不能太多，太多则不利于管理。加密算法太简单则容易找出解密算法，太复杂则导致解密过程耗费时间太多，不利于通信。

一个密码系统要是实际可用的，必须满足如下特性：

（1）每一个加密函数 E 和每一个解密函数 D 都能有效地计算。

（2）破译者取得密文后将不能在有效的时间或成本范围内破解出密钥或明文。

（3）一个密码系统是安全的必要条件——穷举密钥搜索是不可行的，因为密钥空间非常大。

3.1.2 密码学的发展

密码学的发展历程大致经历了三个阶段：古代手工加密阶段、古典机械密码阶段和现代密码学阶段。

1. 古代手工加密阶段

源于应用的无穷需求是推动技术发明和进步的直接动力。存于石刻或史书中的记载表明，许多古代文明，包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。从某种意义上说，战争是密码技术进步的催化剂。人类自从有了战争，就面临着通信安全的需求，密码技术源远流长。

古代手工加密方法大约起源于公元前 440 年出现在古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。

公元前 400 年，斯巴达人发明了“塞塔式密码”，即把长条纸螺旋形地斜绕在一个多棱棒上，将文字沿棒的水平方向从左到右书写，写一个字旋转一下，写完一行再另起一行从左到右写，直到写完。解下来后，纸条上的文字消息杂乱无章、无法理解，这就是密文，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息，这是最早的密码技术。

我国古代的烽火也是一种传递军情的方法。古代的“兵符”就是用来传达信息的密令。

宋曾公亮、丁度等编撰的《武经总要》“字验”记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具有了密本体制的特点。

连闯荡江湖的侠士和被压迫起义者都各自有一套秘密的黑道行话和地下联络的暗语。

2. 古典密码阶段（机械阶段）

古典密码的加密方法一般是文字置换，通过手工或机械变换方式实现。古典密码系统已经初步体现出现代密码体制的雏形，它比古代手工加密方法复杂。

公元前 1 世纪，著名的恺撒（Caesar）密码被用于高卢战争中，这是一种简单易行的单字母代换密码。

公元 9 世纪，阿拉伯的密码学家阿尔 · 金迪（Al’ Kindi，也被称为伊沙克 Ishaq，

801? —873 年,同时还是天文学家、哲学家、化学家和音乐理论家)提出解密的频度分析方法,通过分析计算密文字符出现的频率破译密码。

公元 16 世纪中期,意大利的数学家卡尔达诺(G. Cardano,1501—1576)发明了卡尔达诺漏格板,覆盖在密文上,可从漏格中读出明文,这是较早的一种分置式密码。

公元 16 世纪晚期,英国的菲利普斯(Philips)利用频度分析法成功破解苏格兰女王玛丽的密码信,信中策划暗杀英国女王伊丽莎白,这次解密将玛丽送上了断头台。

1834 年,伦敦大学的实验物理学教授惠斯顿发明了电机,这是通信向机械化、电气化跃进的开始,也为密码通信能够采用在线加密技术提供了前提条件。1881 年世界上的第一个电话保密专利出现。电报、无线电的发明使密码学成为通信领域中不可回避的研究课题。

1914 年第一次世界大战爆发,德俄相互宣战。在交战过程中,德军破译了俄军第一军发给第二军的电文,从中得知,第一军的给养已经中断。根据这一重要情报,德军在这次战役中取得了全胜。这说明当时交战双方已使用电机开展了密码战。

在第一次世界大战进行到关键时刻,英国破译密码的专门机构“40 号房间”利用缴获的德国密码本破译了著名的“齐默尔曼电报”,促使美国放弃中立参战,改变了战争进程。

1918 年,美国数学家吉尔伯特・维那姆发明一次性便笺密码,它是一种理论上绝对无法破译的加密系统,被誉为密码编码学的圣杯。但产生和分发大量随机密钥的困难使它的实际应用受到很大限制,从另一方面来说安全性也更加无法保证。

1920 年,美国电报电话公司的弗纳姆发明了弗纳姆密码。其原理是利用电传打字机的五单位码与密钥字母进行模 2 相加。如若信息码(明文)为 11010,密钥码为 11101,则模 2 相加得 00111 即为密文码。接收时,将密文码再与密钥码模 2 相加得信息码(明文)11010。这种密码结构在今天看起来非常简单,但由于这种密码体制第一次使加密由原来的手工操作进入到由电子电路来实现,而且加密和解密可以直接由机器来实现,因而在近代密码学发展史上占有重要地位。

在第二次世界大战初期,德国使用了一种命名为“恩尼格玛”(Enigma),也称“谜”的密码机,能产生 220 亿种不同的“密钥”组合,如果一个人每分钟测试一个密码,则需要 1.2 万年才能将所有的“密钥”可能组合试完。因此,希特勒完全相信其安全性。盟军对德军加密的信息有好几年一筹莫展,“恩尼格玛”密码机似乎是不可破的。

但是经过盟军密码分析学家的不懈努力,“恩尼格玛”密码机被攻破,英国却获知了“谜”型机的密码原理。英国在伦敦北边一百千米处征集了一块空地,如图 3-2 所示,在那里集结了一大批杰出的数学家、语言学家和象棋大师。其中包括计算机的开山鼻祖图灵(A. Turing)和创办世界上第一个人工智能系统的米基(D. Michie)。他们专门负责截获、破译“谜”型机的密码。由于这个组织的努力,特别是图灵出色的工作,使他们掌握了一整套破译该密码的方法,并完成了一部专门针对“谜”型机的绰号叫“炸弹”的密码破译机,每秒可处理 2000 个字符,几乎可破译截获德国的所有情报。后来又研制出一种每秒可处理 5000 个字符的“巨人”型密码破译机,并投入使用。至此,英方几乎掌握了德国纳粹的绝大多数军事密码和情报,从而掌握了战争的主动权,而德国军方却一无所知。图灵等人为英美联军击败德军做出了突出的贡献。有人估算,如果没有他们的贡献,第二次世界大战

至少还要再打 10 年。




图 3-2　图灵在二战期间英国破译德军密码的基地

在太平洋战争中，由于美国破译了日本海军的九七式机械密码，就在日本舰队司令官山本五十六命令换炸弹的五分钟内，美军在中途岛彻底击溃了日本海军，导致了太平洋战争的决定性转折，日本海军大将山本五十六也因密码电报被美国截获破译而被击毙在飞机上。因此，密码学为战争的胜利立下了大功。

古典密码的代表密码体制主要有单表代换密码、多表代换密码及转轮密码。古典密码体制的主要特点是数据的安全基于算法的保密。

古典密码的发展历史悠久，尽管这些密码比较简单，但它在今天仍有其参考价值。

3. 现代密码学(计算机阶段)

(1) 密码体制模型。

1949 年前密码的研究还称不上是一门科学。直到 1949 年香农在《贝尔系统技术》(bell system technical)杂志上发表了一篇题为“保密系统的通信理论”(communication theory of secrecy system)的著名论文，该文首先将信息论引入了密码，从而把已有数千年历史的密码学推向了科学的轨道，奠定了密码学的理论基础，从而密码成为一门科学。该文利用数学方法对信息源、密钥源、接收和截获的密文进行了数学描述和定量分析，提出了通用的密码体制模型。

需要提出的是，由于受历史的局限，20 世纪 70 年代中期以前的密码学研究基本上是秘密地进行，而且主要应用于军事和政府部门，1949—1975 年这段时间内，密码学的理论进展不大。

(2) 数据加密标准 DES。

密码学的真正蓬勃发展和广泛的应用是从 20 世纪 70 年代中期开始的。这是受计算机科学蓬勃发展刺激和推动的结果。快速电子计算机和现代数学方法一方面为加密技术提供了新的概念和工具，另一方面也给破译者提供了有力武器。计算机和电子学时代的到来给密码设计者带来了前所未有的自由，他们可以轻易地摆脱原先用铅笔和纸进行手工设计时易犯的错误，也不用再面对用电子机械方式实现的密码机的高额费用。

1975 年 1 月 15 日，对计算机系统和网络进行加密的数据加密标准(data encryption standard，DES)由美国国家标准局颁布为国家标准，这是密码术历史上一个具有里程碑意义的事件。

特别是 1977 年美国国家标准局颁布了数据加密标准 DES 用于非国家保密机关，该

系统完全公开了加密、解密算法。此举突破了早期密码学的信息保密的单一目的，使得密码学得以在商业等民用领域广泛应用，从而给这门学科以巨大的生命力。

(3) 公钥密码体制。

在密码学发展的进程中的另一件值得注意的事件是在1976年，美国密码学家迪菲(Diffie)和赫尔曼(Hellman)在一篇题为“密码学的新方向”(new directions in cryptography)一文中提出了一个崭新的思想，建立了著名的公钥密码体制，引发了密码学上的一次革命性的变革。不仅加密算法本身可以公开，甚至加密用的密钥也可以公开。但这并不意味着保密程度的降低。因为如果加密密钥和解密密钥不一样，将解密密钥保密就可以。若存在这样的公钥体制，就可以将加密密钥像电话簿一样公开，任何用户当他想经其他用户传送加密信息时，就可以从这本密钥簿中查到该用户的公开密钥，用它来加密，而接收者能用只有他所具有的解密密钥得到明文。任何第三者不能获得明文。

1978年，由美国麻省理工学院的里维斯特(Rivest)，沙米尔(Shamir)和阿德曼(Ademan)三人提出了RSA公钥密码体制，它是第一个成熟的、迄今为止理论上最成功的公钥密码体制。它的安全性是基于数论中的大整数因子分解。该问题是数论中的一个困难问题，至今没有有效的算法，这使得该体制具有较高的保密性。

公钥密码体制的主要特点是数据的安全基于密钥而不是算法的保密。

1985年，英国牛津大学物理学家戴维·多伊奇(David Deutsch)提出量子计算机的初步设想，这种计算机一旦造出来，可在30秒钟内完成传统计算机要花上100亿年才能完成的大数因子分解，从而破解RSA运用这个大数产生公钥来加密的信息。

1985年，美国的贝内特(Bennet)根据他关于量子密码术的协议，在实验室第一次实现了量子密码加密信息的通信。尽管通信距离只有30cm，但它证明了量子密码术的实用性。与一次性便笺密码结合，同样利用量子的神奇物理特性，可产生连量子计算机也无法破译的绝对安全的密码。

2003，位于日内瓦的Id Quantique公司和位于纽约的MagiQ技术公司，推出了传送量子密钥的距离超越了贝内特实验中30cm的商业产品。市面上已有产品能够将密钥通过光纤传送几十千米。

(4) 认证体制。

按照人们对密码的一般理解，密码是用于将信息加密而不易破译，但在现代密码学中，由于网络的应用，除了信息保密外，还有另一方面的要求，即信息安全体制还要能抵抗对手的主动攻击。所谓主动攻击指的是攻击者可以在信息通道中注入他自己伪造的消息，以骗取合法接收者的相信。主动攻击还可能篡改信息，也可能冒名顶替，这就产生了现代密码学中的认证体制。该体制的目的就是保证用户收到一个信息时，他能验证消息是否来自合法的发送者，同时还能验证该信息是否被篡改。在许多场合中，如电子汇款，能对抗主动攻击的认证体制甚至比信息保密还重要。

(5) 现代密码编码学的特点。

现代密码编码学主要致力于信息加密、信息认证、数字签名和密钥管理方面的研究。信息加密的目的在于将可读信息转变为无法识别的内容，使得截获这些信息的人无法阅读；信息认证的目的在于信息的接收人能够验证接收到的信息是否被敌方篡改或替换过；

数字签名就是使信息的接收人能够确定接收到的信息是否确实是由所希望的发信人发出的；密钥管理是信息加密中最难的部分，因为信息加密的安全性在于密钥。历史上，各国军事情报机构在猎取别国的密钥管理方法上要比破译加密算法成功得多。

（6）现代密码分析学的特点。

现代密码分析学与密码编码学不同，它不依赖数学逻辑的不变真理，必须凭经验，依赖客观世界觉察得到的事实。因而，密码分析更需要发挥人们的聪明才智，更具有挑战性。

现代密码学是一门迅速发展的应用科学。随着因特网的迅速普及，人们依靠它传送大量的信息，但是这些信息在网络上的传输都是公开的。因此，对于关系到个人利益的信息必须经过加密之后才可以在网上传送，这将离不开现代密码技术。

3.1.3 密码技术的应用领域

密码技术是在编码与破译的斗争实践中逐步发展起来的，从手工技术、机械技术到计算机技术，随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。

密码技术有着悠久的历史。在古代密码技术就被用于传递秘密消息。在近代和现代战争中，传递情报和指挥战争均离不开密码技术，外交斗争中也离不开密码技术。

随着计算机和信息技术的发展，密码技术的应用领域不断扩展。密码技术除了用于信息加密外，也用于数据信息签名和安全认证。因此，密码的应用不再局限于为军事、外交斗争服务，它被广泛应用在社会和经济活动中。

具体来说，密码技术主要应用于信息的保密、身份的确认、数据的完整性等领域。

1. 通信中的数据保护

密码技术应用于通信线路上信息的保护。一方面，防止传输中的信息被非法窃听导致失密，另一方面，防止信息的内容被恶意攻击者非法地篡改，并且在发生此类事件后能迅速发现。

2. 存储信息的保护

信息用密码技术加密处理后进行存储，保证只有掌握解密密钥的合法用户才能够存取数据，得到正确的明文。在许多用户的系统中，保护个人秘密、防止文件被破坏。

3. 通信双方的身份验证

密码技术不仅广泛应用于防止传输中的信息和记录存储的信息不被攻击者非法窃听、浏览和篡改，同时，也可以用于识别通信双方的真实性。这种对存取数据和发来电文的对方的合法性进行确证的方法叫“验证”。

4. 非否认性

密码技术还应用于不可否认性服务。它包含对源和目的双方的证明，通常的情况下，

不可否认服务是一种数字签名服务。

除此之外，密码技术还广泛地应用于计算机网络安全领域的其他方面，出现了密码技术应用的社会化和个人化趋势。例如，可以将密码技术应用在电子商务中，对网上交易双方的身份和商业信用进行识别，防止网上电子商务中的“黑客”和欺诈行为；应用于增值税发票中，可以防伪、防篡改，杜绝了各种利用增值税发票偷、漏、逃、骗国家税收的行为，并大大方便了税务稽查；应用于银行支票鉴别中，可以大大降低利用假支票进行金融诈骗的金融犯罪行为；应用于个人移动通信中，大大增强了通信信息的保密性等。

3.1.4 密码学的新概念和新技术

密码学的进一步发展，涌现了大量的新概念和新技术，这里主要介绍零知识证明技术、盲签名、比特承诺和量子密码技术。

1. 密码协议

(1) 协议的含义。

本书中的协议是指两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。协议具有以下三个特征：

① 协议自始至终是有序的过程，每一步骤必须依次执行，在前一步骤没有执行完之前，后面的步骤不可能执行。

② 协议至少需要两个参与者，一个人可以通过执行一系列的步骤来完成某项任务，但它不构成协议。

③ 通过执行协议必须能够完成某项任务。

(2) 协议的特点。

① 协议中的每个人都必须了解协议，并且预先知道所要完成的所有步骤。

② 协议中的每个人都必须同意遵循它。

③ 协议必须是不模糊的，每一步必须明确定义，并且不会引起误解。

④ 协议必须是完整的，对每种可能的情况必须规定具体的动作。

(3) 密码协议。

密码协议，也称作安全协议，是使用密码技术的协议。参与密码协议的人可能是朋友和完全信任的人，也可能是敌人和互相完全不信任的人，相互之间不信任的各方能够在网络上完成这些协议。

密码协议包含某种密码算法，但通常，协议的目的不仅仅是为了简单的秘密性。参与协议的各方可能为了计算一个数值想共享它们的秘密部分，共同产生随机系列，确定互相的身份，或者同时签署合同。在协议中使用密码的目的是防止或发现偷听者和欺骗。

2. 零知识证明

20 世纪 80 年代初，S. Goldwasser 等人提出了零知识证明这一概念。从本质上讲，零知识证明是一种协议。

零知识证明必须包括两个方面，一方为证明者，另一方为验证者。证明者试图向验证

者证明某个论断是正确的，或者证明者拥有某个知识，却不向验证者透露任何有用的消息。

零知识证明目前在密码学中得到了广泛的应用，尤其是在认证协议、数字签名方面，人们利用数字签名设计出了大量优良的算法。

3. 盲签名

盲签名是1982年提出的。盲签名因为具有盲性这一特点，可以有效保护所签署消息的具体内容，所以在电子商务和电子选举等领域有着广泛的应用。

盲签名就是消息拥有者在不让签名者获取所签署消息具体内容的情况下所采取的一种特殊的数字签名技术，它除了满足一般的数字签名条件外，还必须满足下面的两条性质：

(1) 签名者对其所签署的消息是不可见的，即签名者不知道他所签署消息的具体内容。

(2) 签名消息不可追踪，即当签名消息被公布后，签名者无法知道这是他哪次签署的。

盲签名允许消息拥有者先将消息盲化，而后让签名者对盲化的消息进行签名，最后消息拥有者对签字除去盲因子，得到签名者关于原消息的签名。

关于盲签名，可用在文件上进行盲签名做一个直观的说明。

消息盲化就是先将要签名的文件放进信封里，并在信封里的文件上放一张复写纸，当文件在信封中时，任何人不能读它。对文件签名时签名者在信封上签名，他的签名便透过复写纸签到了文件上。除去盲因子就是打开这个信封。

一般来说，一个好的盲签名应该具有以下的性质：

(1) 不可伪造性。除了签名者本人外，任何人都不能以他的名义生成有效的盲签名。这是一条最基本的性质。

(2) 不可抵赖性。签名者一旦签署了某个消息，他无法否认自己对消息的签名。

(3) 盲性。签名者虽然对某个消息进行了签名，但他不可能得到消息的具体内容。

(4) 不可跟踪性。一旦消息的签名公开后，签名者不能确定自己何时签署的这条消息。

满足上面几条性质的盲签名，被认为是安全的。这四条性质既是设计盲签名所应遵循的标准，又是判断盲签名性能优劣的根据。

4. 比特承诺

比特承诺(bit commitment，BC)是密码学中的重要基础协议，其概念最早由1995年图灵奖得主Blum提出。比特承诺方案可用于构建零知识证明、可验证秘密分享、硬币投掷等协议，同时和茫然传送一起构成安全双方计算的基础，是信息安全领域研究的热点。

比特承诺的基本思想如下：发送者张三向接收者李四承诺一个比特 b(如果是多个比特，即比特串 t，则称为比特串承诺)，要求在第1阶段(即承诺阶段)张三向李四承诺这个比特 b，但是李四无法知道 b 的信息；在第2阶段(即揭示阶段)张三向李四证实他在第1

阶段承诺的确实是 b，但是张三无法欺骗李四(即不能在第 2 阶段篡改 b 的值)。

经典环境中关于比特承诺的一个形象的例子：

张三将待承诺的比特或秘密写在一张纸上，然后将这张纸锁进一个保险箱，该保险箱只有唯一的钥匙可以打开。在承诺阶段，张三将保险箱送给李四，但是保留钥匙；到了揭示阶段，张三将比特或秘密告诉李四，同时将钥匙传给李四，使其相信自己的承诺。需要指出的是，保险箱不能被"暴力破解"，甚至允许张三在揭示阶段无须向李四说明承诺的比特或秘密，只要将钥匙发送给李四即可。

一个比特承诺方案必须具备下列性质：

(1) 正确性：如果张三和李四均诚实地执行协议，那么在揭示阶段李四将正确获得张三承诺的比特 b 。

(2) 保密性：在揭示阶段之前李四不能获知 b 的信息。

(3) 绑定性：在承诺阶段结束之后，李四只能在揭示阶段获得唯一的 b。

5. 量子密码技术

量子密码技术是量子物理学和密码学相结合的一门新兴学科，它是利用量子物理学方法实现密码思想的一种新型密码体制。量子密码技术是一种实现保密通信的新方法，它比较于经典密码的最大优势是具有可证明安全性和可检测性。

(1) 量子密码技术的理论基础。

量子密码技术的理论基础是量子力学，而以往密码学的理论基础是数学。与传统密码学不同，量子密码学利用物理学原理保护信息。首先想到将量子物理用于密码技术的是美国科学家威斯纳(Wiesner)。威斯纳在"海森堡测不准原理"和"单量子不可复制定理"的基础上，逐渐建立了量子密码的概念。"海森堡测不准原理"是量子力学的基本原理，指在同一时刻以相同精度测定量子的位置与动量是不可能的，只能精确测定两者之一。"单量子不可复制定理"是"海森堡测不准原理"的推论，它指在不知道量子状态的情况下复制单个量子是不可能的，因为要复制单个量子就只能先作测量，而测量必然改变量子的状态。

(2) 量子密码最基本的原理。

量子密码最基本的原理是"量子纠缠"，即一个特殊的晶体将一个光子割裂成一对纠缠的光子。被爱因斯坦称为"神秘的远距离活动"的量子纠缠，是指粒子间即使相距遥远也是相互联结的。大多数量子密码通信利用的都是光子的偏振特性，这一对纠缠的光子一般有两个不同的偏振方向，就像计算机语言里的"!"和"♯"。根据量子力学原理，光子对中的光子的偏振方向是不确定的，只有当其中一个光子被测量或受到干扰，它才有明确的偏振方向，它代表"!"和"♯"完全是随机的，一旦它的偏振方向被确定，另外一个光子就被确定为与之相关的偏振方向。当两端的检测器使用相同的设定参数时，发送者和接收者就可以收到相同的偏振信息，也就是相同的随机数字串。另外，量子力学认为粒子的基本属性存在于整个组合状态中，所以由纠缠光子产生的密码只有通过发送器和接收器才能阅读。窃听者很容易被检测到，因为他们在偷走其中一个光子时不可避免地要扰乱整个系统。

(3) 当前量子密码技术研究的核心内容。

当前,量子密码技术研究的核心内容是如何利用量子技术在量子通道上安全可靠地分配密钥。在传统的密码术中密钥是指只有通信双方掌握的随机数字串。量子密钥分配的安全性由“海森堡测不准原理”及“单量子不可复制定理”保证。根据这两个原理,即使量子密码不幸被电脑黑客撷取,也因为测量过程中会改变量子状态,黑客得到的会是毫无意义的数据。

可以这样描绘科学家们关于“量子密码”的设想:由电磁能产生的量子(如光子)可以充当为密码解码的一次性使用的“钥匙”。每个量子代表1比特含量的信息,量子的极化方式(波的运动方向)代表数字化信息的数码。量子一般能以四种方式极化——水平的和垂直的,而且互为一组;两条对角线的,也是互为一组。这样,每发送出一串量子就代表一组数字化信息。而每次只送出一个量子,就可以有效地排除黑客窃取更多的解密“钥匙”的可能性。

假如现在有一个窃密黑客开始向“量子密码”动手了,可以看到这样一场有趣的游戏:窃密黑客必须先用接收设施从发射出的一连串量子中吸去一个量子。这时,发射密码的一方就会发现发射出的量子流出现了空格。于是,窃密黑客为了填补这个空格,不得不再发射一个量子。但是,由于量子密码是利用量子的极化方式编排密码的,根据量子力学原理,同时检测出量子的四种极化方式是完全不可能的,窃密黑客不得不根据自己的猜测随便填补一个量子,这个量子由于极化方式的不同很快就会被发现。

(4) 量子密码技术的应用。

量子密码技术的应用分为两类:一是利用量子计算机对传统密码体制的分析;二是利用单光子的测不准原理在光纤一级实现密钥管理和信息加密,即量子密码体制。

量子计算机是一种传统意义上的超大规模并行计算系统,利用量子计算机可以在几秒钟内分解 RSA129 的公钥。根据 Internet 的发展,全光网络将是今后网络连接的发展方向,利用量子技术可以实现传统的密码体制,在光纤一级完成密钥交换和信息加密,其安全性是建立在“海森堡测不准原理”上的,如果攻击者企图接收并检测信息发送方的信息(偏振),则将造成量子状态的改变,这种改变对攻击者而言是不可恢复的,而对收发方则可很容易地检测出信息是否受到攻击。目前量子加密技术仍然处于研究阶段,其量子密钥分配(quantum key distribution,QKD)在光纤上的有效距离还达不到远距离的要求。

(5) 量子密码技术研究现状。

到目前为止,有关量子密码的成果虽然很多,但尚有许多问题有待于深入研究。例如,寻找新的可用量子效应以便提出更多高效的量子密钥分配协议,开发量子加密算法以便形成和完善量子加密理论,在诸如量子身份认证、量子签名等方面改进已有方案或推陈出新,还有研究量子攻击算法和量子密码协议的安全性分析等。

总之,量子密码理论与技术还处于实验和探索之中。

3.2 密码技术的典型加密算法

密码技术是对信息进行加密与解密的技术,加解密技术的核心是加密算法与解密算法,通称为加密算法。加密算法是实施具体加密的基础,它决定了加密的强度、运算量以

及它的实用性。

在计算机出现前，密码算法主要是基于字符的变换，不同的密码算法是字符之间互相代换或者是互相之间换位，好的密码算法是结合这两种方法，每次进行多次运算。现在事情变得复杂多了，但原理还是没变，重要的变化是算法对比特而不是对字母进行变换，实际上这只是字母表长度上的改变，从 26 个元素变为 2 个元素。

加密算法可以通过软件加密与硬件加密两种方式来实现。软件加密通过算法的计算机程序实现，实现简单，成本低，速度比较慢。软件加密相对来说，机密性差。硬件加密通过具体的电子线路实现加密算法，实现复杂，成本高，加密速度比较快。相对软件加密方式，其机密性更好。

本节主要介绍密码技术中典型的古典密码算法、对称密钥算法与公开密钥算法。

3.2.1 古典密码算法

大多数好的密码算法仍然是代换和换位的元素组合。虽然用现代密码学的观点来看，许多古典密码是很不安全的，或者说是极易破解的，但是不能忘记古典密码算法在历史上发挥的重要作用。另外，编制古典密码的技术对于编制现代密码仍然有效，并且古典密码有许多经典的运算方法。

古典密码采用手工或机械操作实现加解密，实现起来相对简单。古典密码大体上可分为两类：代换密码与置换密码。

1. 代换密码

代换是古典密码中用到的最基本的处理技巧。所谓代换，就是将明文中的一个字母由其他字母、数字或符号替代的一种方法。在代换密码中常见的加密算法有单表代换和多表代换。

(1) 单表代换。

单表代换就是明文的一个字符用相应的一个密文字符代替。加密过程中是从明文字母表到密文字母表的一一映射。

设 $A=\{a_0,a_1,\cdots,a_{n-1}\}$ 为明文字母表，$B=\{b_0,b_1,\cdots,b_{n-1}\}$ 为密文字母表，单字符单表替换密码技术使用了 A 到 B 的映射关系为 $f：A\rightarrow B, f(a_i)=b_j$（一般情况下，为保证加密的可逆性，$f$ 是一一映射）将明文中的每一个字母替换为密文字母表中的一个字母。单字符单表替换密码技术的密钥就是映射 f 或密文字母表（一般情况下明文字母表与密文字母表是相同的，这时的密钥就是映射 f）。

(2) 单表代换——棋盘密码。

早在公元前两世纪，一位希腊人提出一种棋盘密码，该密码将 26 个字母放在 5×5 的方格里，i，j 放在一个格子里，具体情况如图 3-3 所示。这样，每个字母就对应了由两个数构成的字符 $\alpha\beta$，α 是该字母所在行的标号，β 是列标号。如 c 对应 13，s 对应 43 等。如果接收到密文为棋盘密码 43 15 13 45 42 15 32 15 43 43 11 22 15 则对应的明文即 secure message。

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

图 3-3 棋盘密码

(3) 单表代换——凯撒密码。

凯撒密码是将英文字母向前推移 k 位。如 $k=5$,则密文字母与明文有如下对应关系。

a b c d e f g h i j k l m n o p q r s t u v w x y z

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

如果收到密文为 XJHZWJRJXXFLJ,则对应明文也为 secure message。此时,k 就是密钥。为了传送方便,可以将 26 个字母一一对应于 0～25 的 26 个整数。如 a 对 0,b 对 1,……,y 对 24,z 对 25。这样凯撒加密变换实际就是一个同余式

$$c = m + k \bmod 26$$

其中 m 是明文字母对应的数,c 是与明文对应的密文的数。

凯撒是率先使用加密函数的古代将领之一,在古罗马的时候他用凯撒密码与其将军们进行联系,因此这种加密算法被称为凯撒密码。

后来,为了提高凯撒密码的安全性,人们对凯撒密码进行了改进,选取 k,b 两个参数,其中要求 k 与 26 互素,明文与密文的对应规则为

$$c = km + b \bmod 26$$

棋盘密码与凯撒密码的密码体制都属于单表代换,是一个明文字母对应一个确定的密文字母。根据这个特点,利用频率分析可以对这样的密码体制进行有效的攻击。方法是在大量的书籍、报刊和文章中,统计各个字母出现的频率。例如,e 出现的次数最多,其次是 t,a,o,I 等。破译者通过对密文中各字母出现频率的分析,结合自然语言的字母频率特征,就可以将该密码体制破译。

(4) 多表代换——维吉尼亚密码。

鉴于单表代换密码体制具有这样的攻击弱点,人们自然就会想办法对其进行改进,来弥补这个弱点,增加抗攻击能力。法国密码学家维吉尼亚(Vigenére)于 1586 年提出一种多表式密码,即一个明文字母可以表示成多个密文字母,通常称为维吉尼亚密码。

其原理是这样的:给出密钥 $K=k[1]k[2]\cdots k[n]$,若明文为 $M=m[1]m[2]\cdots m[n]$,则对应的密文为 $C=c[1]c[2]\cdots c[n]$。

其中 $c[i]=(m[i]+k[i]) \bmod 26$。

例如,若明文 M 为 data security,密钥 $k=$best,将明文分解为长为 4 的序列 data security,对每 4 个字母,用 $k=$best 加密后得密文为 $C=$EELT TIUN SMLR。

从中可以看出,当 K 为一个字母时,就是凯撒密码。而且容易看出,K 越长,保密程度就越高。因为它对每个明文都采用了不同的密钥进行加密,也称为一次一密码技术,它是一种理论上不可破译的密码技术。显然这样的密码体制比单表置换密码体制具有更强的抗攻击能力,而且其加密、解密均可用所谓的维吉尼亚方阵来进行,从而在操作上简单易行。该密码曾被认为是三百年内破译不了的密码,因而这种密码在今天仍被使用着。

2. 置换密码

把明文中的字母或数字重新排列,字母或数字本身不变,但顺序被打乱了,位置发生了改变,这样所编成的密码称为置换密码,又称换位密码。

置换只不过是一个简单的换位，每个置换都可以用一个置换矩阵 E_k 来表示。每个置换都有一个与之对应的逆置换 D_k。置换密码的特点是仅有一个发送方和接受方知道的加密置换（用于加密）及对应的逆置换（用于解密）。它是对明文 L 长字母组中的字母位置进行重新排列，而每个字母本身并不改变。

例如：

明文：zhe shi zhi huan mi ma

密文：ami mna uhi hzih se hz

可以看出，这是一种倒序的置换密码，显然安全性很弱，很容易被破译。

又例如，可以把明文按某一顺序排成一个矩阵，然后按另一顺序选出矩阵中的字母以形成密文，最后组成固定长度的字母作为密文。

置换密码很简单，比单表代换密码还简单。因为本身是不变的，只是位置变了，所以很容易用穷举法破译。

3.2.2　对称密钥算法

对称密钥算法又叫专用密钥算法，即发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算，加密密钥能够从解密密钥中推算出来，反过来也成立。通常说来，对称密钥算法简单高效，密钥简短，难以破译。但是，在网络环境下存在相应的不安全性。

对称密钥算法主要包括 DES、3DES、IDEA、AES 等。对称密钥算法也称为对称密钥密码体制。

1. 数据加密标准（data encryption standard，DES）

DES 是由 IBM 公司研制的加密算法，其算法较复杂，但易于实现。它只对小的分组进行简单的逻辑运算，用硬件和软件实现起来都比较容易，是迄今为止使用最为广泛的加密算法，已经有 30 多年的历史。1977 年 1 月，DES 被正式批准为美国联邦信息处理标准，作为商业和非保密信息的加密标准被广泛采用，直到 1998 年 12 月才被 AES（advanced encryption standard，高级加密标准）取代。尽管如此，DES 对推进密码理论的发展和应用仍起到了重要的作用。

（1）DES 算法的描述。

DES 算法将信息分成 64 位的分组，并使用 56 位长度的密钥。它对每一个分组使用一种复杂的变位组合、替换，再进行异或运算和其他一些过程，最后生成 64 位的加密数据。对每一个分组进行 19 步处理，每一步的输出是下一步的输入。如图 3-4 所示为 DES 算法的加密流程。

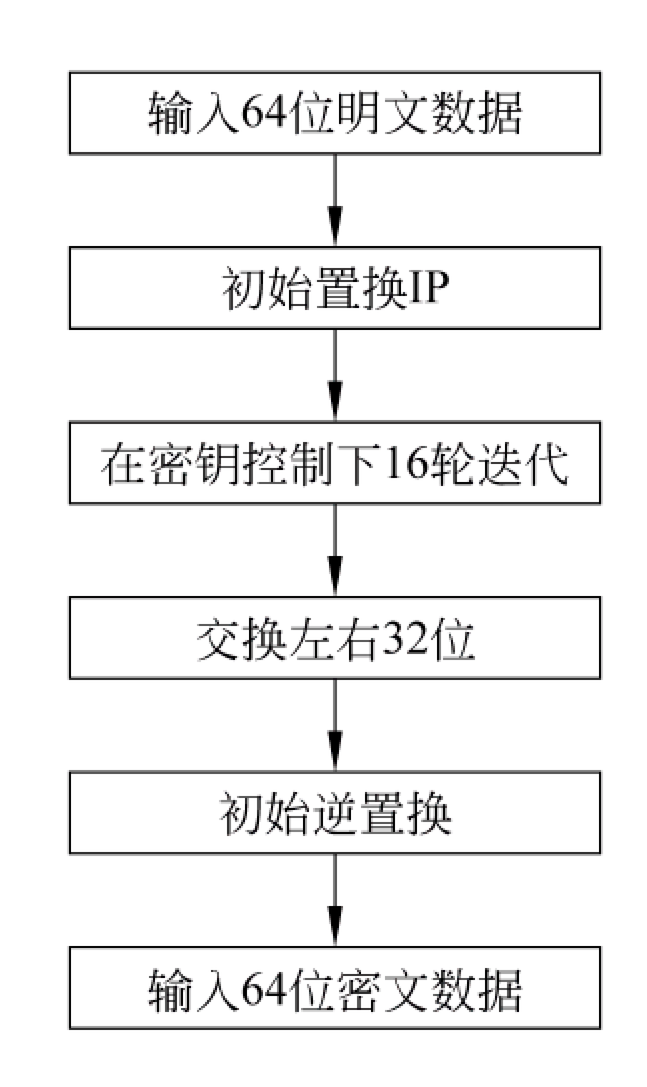


图 3-4　DES 算法加密流程

（2）DES 算法的安全性。

DES 算法的加密和解密密钥相同，属于一种对称加密技术。对称加密技术从本质上说都是使用替代密码和换位密码

进行加密的。

（3）DES 的破译。

DES 使用 56 位密钥对 64 位的数据块进行加密，并对 64 位的数据块进行 16 轮编码。在 1977 年，人们估计要耗资两千万美元才能建成一个专门计算机用于 DES 的解密，而且需要 12 个小时的破解才能得到结果。所以，当时 DES 被认为是一种十分强壮的加密方法。但今天，只需二十万美元就可以制造一台破译 DES 的特殊的计算机，所以现在 DES 对要求“强壮”加密的场合已经不再适用了。

2. 3DES

3DES 又称 Triple DES，是三重数据加密算法（triple data encryption algorithm，TDEA）块密码的通称，是 DES 加密算法的一种模式，它使用 3 条 56 位的密钥对数据进行三次加密。它相当于是对每个数据块应用三次 DES 加密算法。由于计算机运算能力的增强，DES 密码的密钥长度变得容易被暴力破解，3DES 即设计用来提供一种相对简单的方法，即通过增加 DES 的密钥长度来避免类似的攻击，而不是设计一种全新的块密码算法。比起最初的 DES，3DES 更为安全。3DES 是 DES 向 AES 过渡的加密算法，是 DES 的一个更安全的变形。

3DES 以 DES 为基本模块，通过组合分组方法设计出分组加密算法，其具体实现如下：

设 $E_k()$ 和 $D_k()$ 代表 DES 算法的加密和解密过程，k 代表 DES 算法使用的密钥，P 代表明文，C 代表密文，则

3DES 加密过程为：$C=E_{k3}(D_{k2}(E_{k1}(P)))$

3DES 解密过程为：$P=D_{k1}(E_{k2}(D_{k3}(C)))$

也就是说，加密过程使用 k_1 为密钥进行 DES 加密，再用 k_2 为密钥进行 DES 解密，最后以 k_3 进行 DES 加密。而解密则为其反过程：即以 k_3 解密，以 k_2 加密，最后以 k_1 解密。每次加密操作都只处理 64 位数据，称为一块。无论是加密还是解密，中间一步都是前后两步的逆。

k_1、k_2、k_3 决定了算法的安全性，若三个密钥互不相同，本质上就相当于用一个长为 168 位的密钥进行加密。多年来，它在对付强力攻击时是比较安全的。若数据对安全性要求不那么高，k_1 可以等于 k_3。在这种情况下，密钥的有效长度为 112 位。

3. IDEA 算法

IDEA（international data encryption algorithm）是在 1991 年由瑞士联邦技术协会的 Xuejia Lai 和 James Massey 开发的。IDEA 以 64 位的明文块进行分组，密钥长度为 128 位，主要采用 3 种运算：异或、模加、模乘。

因为 IDEA 算法的密钥长度为 128 位，是 DES 密钥长度的两倍。它能够抵抗差分密码分析方法和相关密钥分析方法的攻击。科学家已证明 IDEA 算法在其 8 轮迭代的第 4 轮之后便不受差分密码分析的影响了。假定穷举法攻击有效的话，那么即使设计一种每秒钟可以试验 10 亿个密钥的专用芯片，并将 10 亿片这样的芯片用于此项工作，仍需 1013 年才能解决问题。目前，尚无一篇公开发表的试图对 IDEA 进行密码分析的文章。

因此，目前，应当说 IDEA 是一种安全性好、效率高的分组密码算法。

4. 高级加密标准（advanced encryption standard，AES）

AES 是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。美国国家标准与技术研究院（NIST）于 2001 年 11 月 26 日公开发布，并在 2002 年 5 月 26 日使其成为有效的标准。目前 AES 已成为对称密钥加密中最流行的算法之一。该算法为比利时密码学家 Joan Daemen 和 Vincent Rijmen 所设计，结合两位作者的名字，所以 AES 又称 Rijndael 加密法。

AES 的基本要求是，采用对称分组密码体制，加密数据块长度固定为 128 位，密钥长度可以是 128 位、192 位、256 位中的任意一个。

AES 加密有很多轮的重复和变换，加密过程如图 3-5 所示。

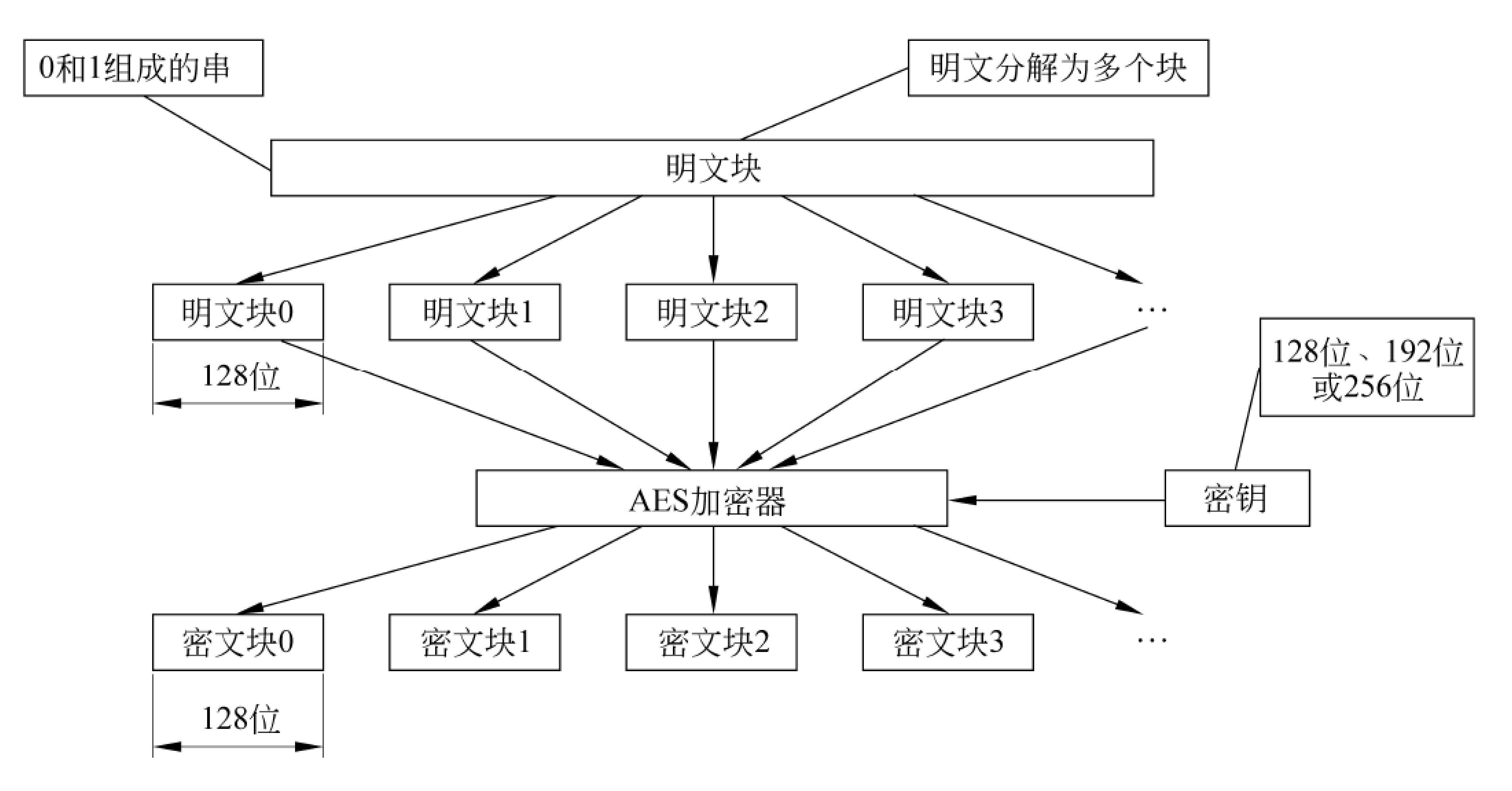


图 3-5　AES 加密过程

3.2.3　公开密钥算法——RSA 算法及应用

1. 公开密钥算法

公开密钥算法也称非对称密钥算法，是现代密码学的最重要的成果。传统密码学重点研究如何保护敏感的通信，这只是当今密码学主题研究的一个方面，对信息发送人的身份验证，是当今密码学主题研究的另一个方面，公开密钥算法为这两方面的问题都给出了良好的解决方案。

与公开密钥算法对应的是对称密钥算法，由于对称密钥双方使用的是相同的密钥，在当今公开的计算机网络上安全地传送和保管密钥成为一个严峻的问题，1976 年，Diffie 和 Hellman 为解决密钥安全问题，在他们的"密码学的新方向"一文中，提出了一种密钥交换协议，允许在不安全的媒体上通信双方交换信息，安全地达成一致的密钥。在此新思想的基础上，很快出现了不对称密钥算法，即公开密钥算法（public-key algorithm）。其中，收

信方和发信方使用的密钥互不相同，而且几乎不可能由加密密钥推导出解密密钥。

由于加密密钥不同于解密密钥，加密密钥可以公之于众，谁都可以用，称为“公开密钥（公钥）”；解密密钥只有解密人自己知道，称为“秘密密钥（私钥）”。公开密钥算法也称为公开密钥密码体制。

2. RSA 公开密钥算法

RSA 公开密钥算法是 1977 年由 Ron Rivest、Adi Shamirh 和 LenAdleman 在（美国麻省理工学院）开发的。RSA 的取名就是来自于这三位发明者的姓的第一个字母。后来，他们在 1982 年创办了以 RSA 命名的公司 RSA Data Security Inc. 和 RSA 实验室，该公司和实验室在公开密钥密码系统的研究和商业应用推广方面具有举足轻重的地位。

RSA 是当今最有影响力的公开密钥算法，它能够抵抗到目前为止已知的所有密码攻击，已被 ISO 推荐为公钥数据加密标准。目前，RSA 被广泛应用于各种安全和认证领域，如 Web 服务器和浏览器信息安全、E-mail 的安全和认证、对远程登录的安全保证和各种电子信用卡系统等。

RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。

1977 年，《科学的美国人》（Scientific American）杂志悬赏征求分解一个 129 位十进数（426 位二进制数），直至 1994 年 3 月，才由 Atkins 等人在因特网上动用了 1600 台计算机，前后花了八个月的时间，找出了答案。然而，这种“困难性”在理论上至今未能严格证明，但又无法否定。对于许多密码研究分析人员和数学家而言，因式分解问题的“困难性”仍是一种信念，一种有一定根据的合理的信念。

3. RSA 实现原理

RSA 实现原理如图 3-6 所示，在节点 B 随机生成密钥 e 作为公有密钥，再由 e 计算出另一个密钥 d 作私有密钥。

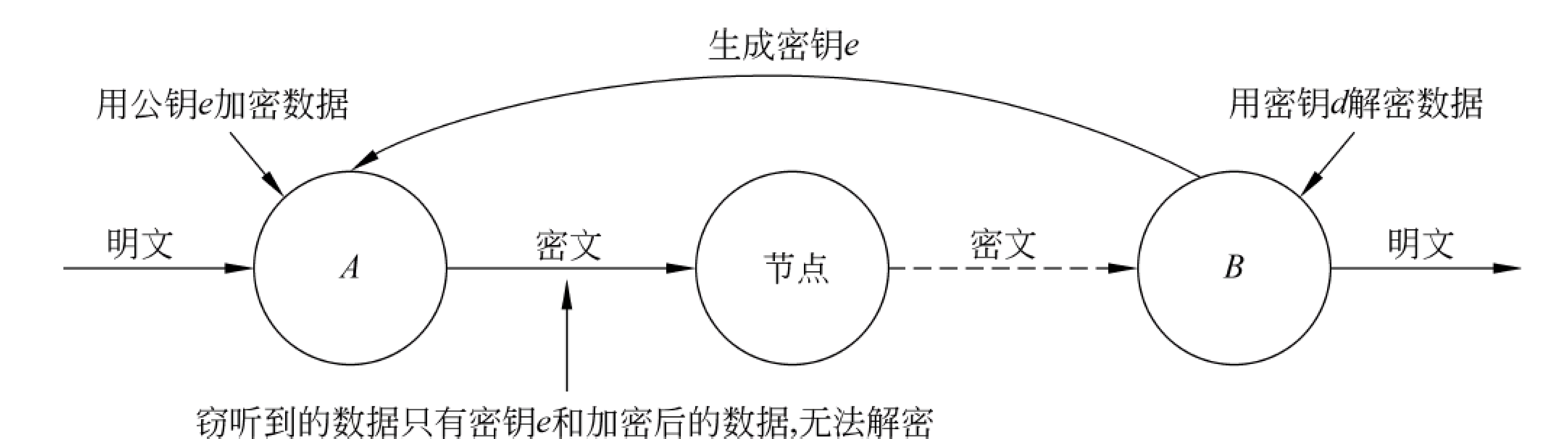


图 3-6 RSA 实现原理

4. RSA 算法的加密过程

RSA 算法加密过程的具体步骤如下：

（1）为字母制定一个简单的编码，如 A～Z 分别对应 1～26。

(2) 选择一个足够大的数 n,使 n 为两个大的素数(只能被 1 和自身整除的数)p 和 q 的乘积。为便于说明,在此使用 $n=p\times q=3\times 11=33$。

(3) 找出一个数 k,k 与 $(p-1)\times(q-1)$ 互为素数。此例中选择 $k=3$,与 $2\times 10=20$ 互为素数。数字 k 就是加密密钥。根据数论中的理论,这样的数一定存在。

(4) 将要发送的信息分成多个部分,一般可以将多个字母分为一部分。在此例中将每一个字母作为一部分。若信息是"SUZAN",则分为 S、U、Z、A 和 N。

(5) 对每一部分,将所有字母的二进制编码串接起来,并转换成整数。在此例中各部分的整数分别为 19、21、26、1 和 14。

(6) 将每个部分扩大到它的 k 次方,并使用模 n 运算,得到密文。在此例中分别是 193mod33=28,213 mod 33=21,263 mod 33=20,13 mod 33=1 和 143 mod 33=5。接收方收到的加密信息是 28、21、20、1 和 5。

5. RSA 算法的解密过程

(1) 找出一个数 k' 使得 $k\times k'-1=0 \bmod ((p-1)\times(q-1))$,即 $k\times k'-1$ 能被 $(p-1)\times(q-1)$ 整除。k′的值就是解密密钥。在此例中选择 $k'=7$,$3\times 7-1=20$,$(p-1)\times(q-1)=20$,能被整除。

(2) 将每个密文扩大到它的 k' 次方,并使用模 n 运算,可得到明文。在此例中分别为 287 mod 33=9217 mod 33=21207 mod 33=26,17 mod 33=1 和 57 mod 33=14。接收方解密后得到的明文的数字是 19、21、26、1 和 14,对应的字母是 S、U、Z、A 和 N。

6. RSA 算法的安全性

RSA 算法的安全性取决于从公开密钥 (n,k) 计算出秘密密钥 (n,k')。n 和 k 以及算法都是公开的。在已知 n 和 k 的情况下是否容易或很快求出 k',是衡量 RSA 算法安全性的关键因素。

在已知 n 和 k 的情况下求 k' 的关键是对 n 因式分解,找出 n 的两个素数 p 和 q。因此,寻求有效的因式分解的算法就是寻求一把锐利的"矛",来击穿 RSA 公开密钥算法这个"盾"。数学家和密码学家们一直在刻苦努力寻求更锐利的"矛"和更坚固的"盾",而且不仅限于 RSA 一种方案。对 RSA 来说,加厚"盾"即 n 取更大的值。所以,RSA 算法的安全,需要选择 n 的大小,也就意味着密钥的长度要足够长,密钥长度越长,安全性越高。

由于高速计算机的出现,RSA 实验室认为,以前已经很具有安全性的 512 位密钥长度已经不够安全。1997 年,RSA 组织公布的密钥长度标准是:个人使用 768 位密钥,公司使用 1024 位密钥,而一些非常重要的机构使用 2048 位密钥。总之,随着硬件资源的迅速发展和因数分解算法的不断改进,为保证 RSA 的安全性,最实际的做法是不断增加模 n 的位数。

7. 公开密钥算法与对称密钥算法的比较

公开密钥算法与对称密钥算法相比较,确实有其不可取代的优点,但它的运算量远大于后者,超过几百倍、几千倍甚至上万倍,复杂得多。

在网络上全都用公开密钥密码体制来传送机密信息是没有必要的，也是不现实的。在计算机系统中使用对称密钥密码体制已有多年，既有比较简便可靠的，久经考验的方法，如以DES为代表的分块加密算法（及其扩充DESX和3DES），也有一些新的方法发表，如RC2、RC4、RC5等，其中RC2和RC5是分块加密算法，RC4是数据流加密算法。

在传送机密信息的网络用户双方，如果使用某个对称密钥算法，如DES，同时使用RSA来传送DES的密钥，就可以综合发挥两种算法的优点，即DES高速简便性和RSA密钥管理的方便和安全性。

公开密钥算法与对称密钥算法的比较如表3-1所示。

表3-1　公开密钥算法与对称密钥算法的比较

	对称密钥算法	公开密钥算法
密钥个数	1个	2个
算法速度	较快	较慢
算法对称性	对称，解密密钥可以从加密密钥中推算出来	不对称，解密密钥不能从加密密钥中推算出来
应用领域	数据的加密和解密	对数据进行数字签名、确认、鉴定、密钥管理和数字封装等
典型算法	DES、3DES、RC2、RC4、IDEA和Skipjack等	Diffie-Hellman、RSA、椭圆曲线加密等
一般要求	1. 加密解密用相同密钥 2. 收发双方必须共享密钥	1. 加密解密算法相同，但使用不同密钥 2. 发送方拥有公钥，接收方拥有私钥
安全性要求	1. 密钥必须保密 2. 没有密钥，解密不可行	1. 解密密钥（私钥）必须保密 2. 无私钥，解密不可行 3. 知道算法和公钥以及若干密文不能确定私钥

3.3　密码技术的应用

本节主要介绍解密技术在实际中的应用，例如数字签名、数字摘要、数字证书等。

3.3.1　数字签名

1. 什么是数字签名

数字签名是非对称密钥加密技术与单向Hash函数技术的典型应用。数字签名是通过一个单向函数对要传送的报文进行处理得到的，用于认证报文来源并核实报文是否发生变化的一个字母数字串。

2. 数字签名的作用

数字签名可以起到与手写签字或印章同样的法律效用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和或其他与数据内容有关的变量进行加密处理，

完成对数据的合法"签名",数据接收方则利用对方的公钥来解读收到的"数字签名",并将解读结果用于对数据完整性的检验,以确认签名的合法性。

3. Hash 函数的概念

Hash 一般翻译做"散列",直接音译为"哈希",就是把任意长度的输入(又叫做预映射,pre-image),通过散列算法,变换成固定长度的输出,该输出就是散列值。简单地说,就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

在信息安全技术中,经常需要验证消息的完整性,Hash 函数提供了这一服务,它对不同长度的输入消息,产生固定长度的输出。这个固定的长度的输出称为原输入消息的"散列"或"消息摘要"(message digest)。一个安全的哈希函数 H 必须具有以下属性:

(1) H 就够应用到大小不一的数据上。

(2) H 能够生成大小固定的输出。

(3) 对于任意给定的 x,H(x)的计算相对简单。

(4) 对于任意给定的代码 h,要发现满足 H(x)=h 的 x 在计算上是不可行的。

(5) 对于任意给定的块 x,要发现满足 H(y)=H(x)而 y=x 在计算上是不可行的。

(6) 要发现满足 H(x)=H(y)的(x,y)对在计算上是不可行的。

4. 数字签名的要求

类似于手写签字,数字签名应满足以下要求:

(1) 接收方能够确认或证实发送方的签字,但不能伪造;

(2) 发送方发出签字的消息给接收方后就不能否认它所签发的消息;

(3) 接收方对收到的签字消息不能否认;

(4) 第三者可以确认收发双方之间的消息传送,但不能伪造这一过程。

5. 不同类型的数字签名

(1) 使用对称密钥算法的数字签名。

由于这种方法是逐位进行签名的,所以只要有一位被改动过,接受方就得不到正确的数字签名,因此其安全性较好。

其缺点是:签名太长,签名密钥及相应的验证信息不能重复使用,否则极不安全。

(2) 使用非对称密钥密码算法的数字签名。

非对称密钥密码算法使用两个密钥:公开密钥和私有密钥,分别用于对数据的加密和解密,即如果用公开密钥对数据进行加密,只有用对应的私有密钥才能进行解密。如果用私有密钥对数据进行加密,则只有用对应的公开密钥才能解密。使用公钥密码算法进行数字签名的加密标准有 RSA、DSA、Diffie-Hellman 等。

其签名和验证过程为:发送方首先用公开的单向函数对报文进行一次变换,得到数字签名,然后利用私有密钥对数字签名进行加密后,附在报文之后一同发出。接收方用发送方的公开密钥对数字签名进行解密交换,得到一个数字签名的明文。发送方的公钥可以由一个可信赖的技术管理机构,即认证中心(certificate authority,CA)发布。接收方将

得到的明文通过单向函数进行计算，同样得到一个数字签名，再将两个数字签名进行对比。如果相同，则证明签名有效，否则无效。

(3) 使用报文摘要算法的数字签名。

报文摘要是最主要的数字签名方法。该数字签名方法是将数字签名与要发送的信息紧密联系在一起，它更适合于电子商务活动。使用报文摘要算法进行数字签名的通用加密标准有：SHA-1 和 MD5 等。下面以 MD5 为例简要说明。

MD5 是目前应用最广泛的报文摘要算法，可以为每个文件生成一个数字签名。MD5 属于一种 Hash 函数，其定义为：算法以一个任意长信息作为输入，产生一个 128 位的“指纹”或“摘要信息”。

MD5 提供了一种单向的 Hash 函数，是一种校验工具。它将一个任意长的字串作为输入，产生一个 128 位的“报文摘要”，附在信息报文后面，以防报文被篡改。MD5 被认为对两个不同报文产生相同的报文摘要是不可计算的，并且对一个已给定的报文摘要，对另一个报文产生同样的报文摘要也是不可计算的。

在计算机安全中，MD5 算法是一种非常有效的对付特洛伊木马程序的工具。通过 MD5 算法计算每个文件的数字签名可以检查文件是否被更换或是否与原来的一致。

6. 公钥密码体制实现数字签名的流程

如假设 A 要发送一个电子文件给 B，A、B 双方只需经过下面的三个步骤即可：

(1) A 用其私钥加密文件，这便是签字过程；

(2) A 将加密的文件送到 B；

(3) B 用 A 的公钥解开送来的文件。

3.3.2 数字摘要

1. 什么是数字摘要

数字摘要技术就是单向 Hash 函数技术，也称作数字指纹，利用单向散列(Hash)函数把任意长度的明文输入映射为固定长度(如 128 位)的密文输出，这个固定长度的密文输出就叫做消息摘要。

2. 数字摘要的作用

数字摘要是将任意长度的消息变成固定长度(128 位)的短消息，由一个单项 Hash 函数对消息进行作用而产生。对于数字签名来说，是用来处理短消息的，而相对于较长的消息则显得有些吃力，所以对于较长的消息进行加密处理则采用数字摘要更为简便。如果消息在传递的途中改变，则接受者通过对收到消息新产生的摘要与原摘要比较，就可知道信息是否被改变。因此数字摘要可以判定出消息的完整性。

3. 数字摘要的安全性

一个 Hash 函数的好坏是由发生碰撞的概率决定的。如果攻击者能够轻易地构造出

两个消息具有相同的Hash值，那么这样的Hash函数是很危险的。一般来说，安全Hash标准的输出长度为160位，这样才能保证它足够安全。这一加密方法亦称为安全Hash编码法(secure hash algorithm，SHA)或MD5(MD standards for message digest)，由Ron Rivest所设计。该编码法采用单向Hash函数将需加密的明文"摘要"成一串128位的密文，这一串密文亦称为数字指纹(finger print)，它有固定的长度，且不同的明文摘要成密文，其结果总是不同的，而同样的明文其摘要必定一致。这样这摘要便可成为验证明文是否是"真身"的"指纹"了。

4. 数字摘要基本流程

数字摘要的基本流程是：

(1) 被发送文件用SHA编码加密产生128位的数字摘要。

(2) 发送方用自己的私用密钥对摘要再加密，这就形成了数字签名。

(3) 将原文和加密的摘要同时传给对方。

(4) 对方用发送方的公共密钥对摘要解密，同时对收到的文件用SHA编码加密产生又一个摘要。

(5) 将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比。如果两者一致，则说明传送过程中信息没有被破坏或篡改过。

3.3.3 数字时间戳

1. 什么是数字时间戳

数字时间戳(digital time-stamp)可以算作数字签名应用的一种变种，在交易文件的书面合同中，文件签署的日期和签名一样都是十分重要的。在电子交易中，数字时间戳对电子文件发表的日期和时间信息提供安全保护。

2. 数字时间戳的作用

数字时间戳解决了数字签名有效性的问题和数据电文容易被篡改伪造、产生时间不确定的问题，为电子文件发表时间提供了安全保护和证明。

3. 数字时间戳的组成

数字时间戳是网上安全服务项目，由专门的机构提供。时间戳是一个经加密后形成的凭证文档，它包括三个部分：

(1) 需要加时间戳的文件的摘要；

(2) 数字时间戳机构收到文件的日期和时间；

(3) 数字时间戳机构的数字签名。

4. 数字时间戳的基本流程

数字时间戳的基本过程为：

(1) 用户首先将需要加时间戳的文件用 Hash 编码加密形成摘要；

(2) 将该摘要发送到数字时间戳机构；

(3) 数字时间戳机构在加入收到文件摘要的日期和时间信息后再对该文件加密，送回用户。

3.3.4 数字证书

1. 什么是数字证书

数字证书是一种权威性的电子文档，由权威公正的第三方机构，即 CA 中心签发的证书。它以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性。

2. 数字证书的作用

使用了数字证书，即使发送的信息在网上被他人截获，甚至丢失了个人的账户、密码等信息，仍可以保证账户、资金安全。它能提供在 Internet 上进行身份验证的一种权威性电子文档，人们可以在互联网交往中用它来证明自己的身份和识别对方的身份。当然在数字证书认证的过程中证书认证中心(CA)作为权威的、公正的、可信赖的第三方，其作用是至关重要的。如何判断数字认证中心公正第三方的地位是权威可信的，国家工业和信息化部以资质合规的方式，陆续向天威诚信数字认证中心等 30 家相关机构颁发了从业资质。

3. 数字证书的应用范围

数字证书可用于发送安全电子邮件、访问安全站点、网上证券交易、网上招标采购、网上办公、网上保险、网上税务、网上签约和网上银行等安全电子事务处理和安全电子交易活动。

4. 数字证书的原理

数字证书里存有很多数字和英文，当使用数字证书进行身份认证时，它将随机生成 128 位的身份码，每份数字证书都能生成相应但每次都不可能相同的数码，从而保证数据传输的保密性，即相当于生成一个复杂的密码。

数字证书绑定了公钥及其持有者的真实身份，它类似于现实生活中的居民身份证，所不同的是数字证书不再是纸质的证照，而是一段含有证书持有者身份信息并经过认证中心审核签发的电子数据，可以更加方便灵活地运用在电子商务和电子政务中。

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥(私钥)，用它进行解密和签名；同时设定一把公共密钥(公钥)并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，

即只有用私有密钥才能解密。在公开密钥密码体制中，常用的一种是RSA体制。其数学原理是将一个大数分解成两个质数的乘积，加密和解密用的是两个不同的密钥。即使已知明文、密文和加密密钥（公开密钥），想要推导出解密密钥（私密密钥），在计算上是不可能的。按现在的计算机技术水平，要破解目前采用的1024位RSA密钥，需要上千年的计算时间。公开密钥技术解决了密钥发布的管理问题，商户可以公开其公开密钥，而保留其私有密钥。购物者可以用人人皆知的公开密钥对发送的信息进行加密，安全地传送给商户，然后由商户用自己的私有密钥进行解密。

用户也可以使用自己的私钥对信息加以处理，由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。采用数字签名，能够确认以下两点：

（1）保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

（2）保证信息自签发后到收到为止未曾作过任何修改，签发的文件是真实文件。

数字证书里存有很多数字和英文，当使用数字证书进行身份认证时，它将随机生成128位的身份码，每份数字证书都能生成相应但每次都不可能相同的数码，从而保证数据传输的保密性，即相当于生成一个复杂的密码。

数字证书绑定了公钥及其持有者的真实身份，它类似于现实生活中的居民身份证，所不同的是数字证书不再是纸质的证照，而是一段含有证书持有者身份信息并经过认证中心审核签发的电子数据，可以更加方便灵活地运用在电子商务和电子政务中。

5. 数字证书的颁发过程

数字证书颁发过程一般为：用户首先产生自己的密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户发送而来，然后，认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。数字证书由独立的证书发行机构发布。数字证书各不相同，每种证书可提供不同级别的可信度。可以从证书发行机构获得您自己的数字证书。

6. 数字证书的特性

数字证书具有以下几种特性：

（1）信息的保密性：交易中的商务信息均有保密的要求。如信用卡的账号和用户名被人知悉，就可能被盗用；订货和付款的信息被竞争对手获悉，就可能丧失商机。因此在电子商务的信息传播中均有加密的要求。

（2）交易者身份的确定性：网上交易的双方很可能素昧平生，相隔千里。要使交易成功首先要能确认对方的身份，对商家要考虑客户端不能是骗子，而客户也会担心网上的商店不是一个玩弄欺诈的黑店。因此能方便而可靠地确认对方身份是交易的前提。对于为顾客或用户开展服务的银行、信用卡公司和销售商店，为了做到安全、保密、可靠地开展服务活动，都要进行身份认证的工作。对有关的销售商店来说，他们对顾客所用的信用卡的号码是不知道的，商店只能把信用卡的确认工作完全交给银行来完成。银行和信用卡

公司可以采用各种保密与识别方法，确认顾客的身份是否合法，同时还要防止发生拒付款问题以及确认订货和订货收据信息等。

（3）不可否认性：由于商情的千变万化，交易一旦达成是不能被否认的。否则必然会损害一方的利益。例如订购黄金，订货时金价较低，但收到订单后，金价上涨了，如收单方能否认受到订单的实际时间，甚至否认收到订单的事实，则订货方就会蒙受损失。因此电子交易通信过程的各个环节都必须是不可否认的。

（4）不可修改性：交易的文件是不可被修改的，如上例所举的订购黄金，供货单位在收到订单后，发现金价大幅上涨了，如其能改动文件内容，将订购数 1 吨改为 1 克，则可大幅受益，那么订货单位可能就会因此而蒙受损失。因此电子交易文件也要能做到不可修改，以保障交易的严肃和公正。

3.3.5 密码技术其他应用

1. 数字水印

数字水印（digital watermarking）技术是将一些标识信息（即数字水印）直接嵌入数字载体当中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改，但可以被生产方识别和辨认。通过这些隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是信息隐藏技术的一个重要研究方向。数字水印是实现版权保护的有效办法，是信息隐藏技术研究领域的重要分支。

2. 数字指纹

数字指纹（digital fingerprinting）是指与用户和某次购买过程有关的信息。当发行商发现被非法分发行为时，可以根据该信息对进行非法分发的用户实现跟踪。

数字指纹体制主要由两部分构成，一部分是用于向复制中嵌入指纹并对带指纹复制进行分发的复制分发体制；另一部分是实现对非法分发者进行跟踪并审判的跟踪体制。往往上述两部分通过发行商、用户（还可能有登记中心、审判者等实体）之间的一系列协议实现，因此数字指纹体制也可以分为算法和协议两部分。

其中，算法包括指纹的编码和解码、指纹的嵌入和提取以及复制的分发策略等内容，而协议部分则规定了各实体之间如何进行交互以实现具有各种特点的复制分发和跟踪体制（如实现用户的匿名性等）。

3. 数字身份证

数字身份证是指将真实身份信息浓缩为数字代码，可通过网络、相关设备等查询和识别的公共密钥。ORC（official release code，ORC）通过与公安部身份查询渠道与身份证信息绑定，并实现相关证件的第三方核实验证，免费网络查询，是目前最完善的数字身份证之一，在商务合作、交友、消费、求职等领域得到广泛的应用。

3.4　应用实例

3.4.1　Office 文件的加密与解密

在计算机日常使用中，Word 文件是使用最多的数据文件，当文件需要进行简单加密的时候，可以利用 Word 自带的加密选项对所需文件进行加密。文件加密后，长时间不用导致忘记文件密码不能打开，可以利用解密软件进行解密。

下面通过实例说明 Office 文件加密与解密的方法。

1. Office 文件的加密过程

第 1 步：使用 Word 创建 secTest.doc 文件，如图 3-7 所示。

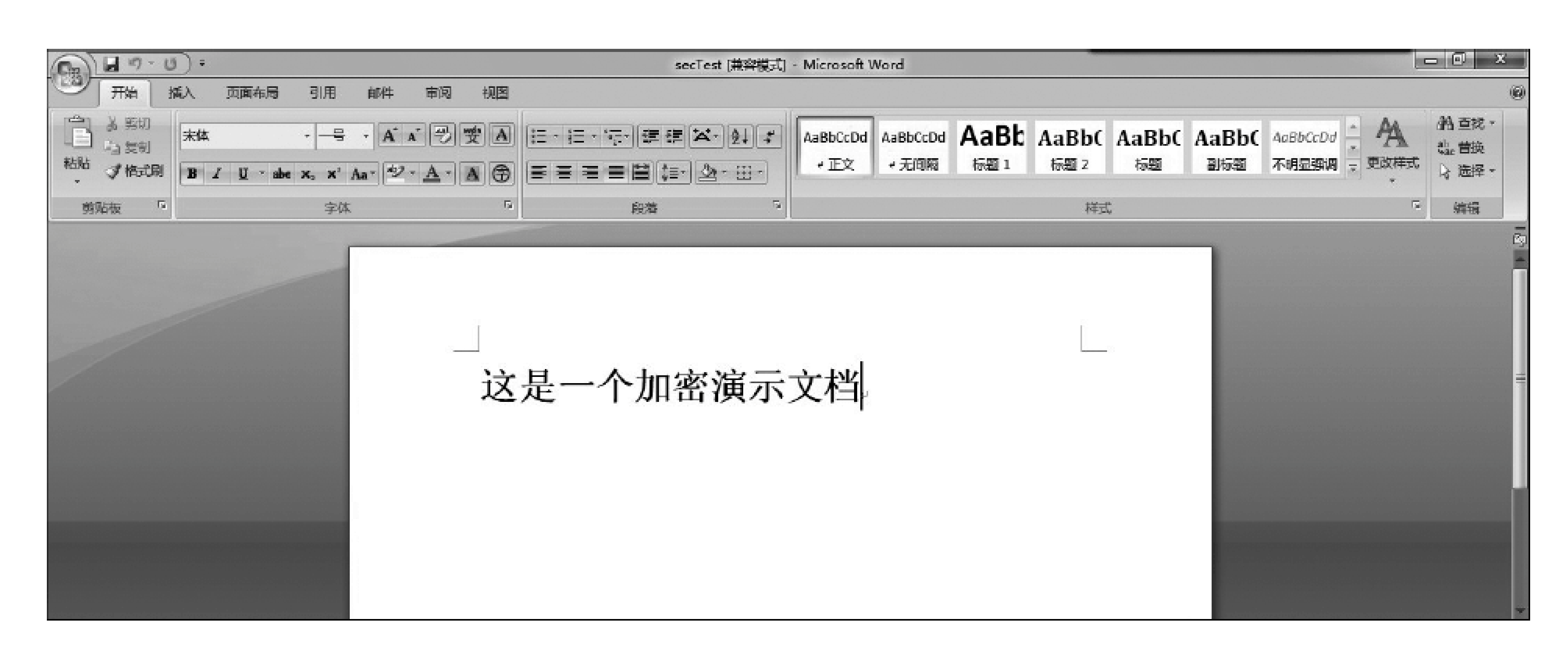


图 3-7　创建 secTest.doc 文件

第 2 步：设置密码。

(1) 在 Word 文档创建界面，单击左上角 Office 图标，选择“另存为”→“Word 97-2003 文档”命令菜单，打开“另存为”对话框，如图 3-8 所示。



图 3-8　“另存为”对话框

(2) 在图 3-8 中单击对话框左下角【工具】按钮，选择“常规选项”命令菜单，如图 3-9 所示。

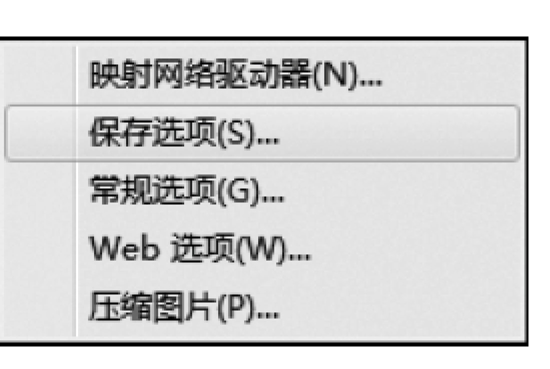


图 3-9 “常规选项”命令菜单

(3) 打开“常规选项”对话框，分别设置打开文件时的密码和修改文件时的密码，如图 3-10 所示，最后单击【确定】按钮。

第 3 步：输入密码。

双击 secTest. doc 文件时，会依次出现要求打开文件的密码和修改文件的密码，如图 3-11、图 3-12 所示。



图 3-10 “常规选项”对话框



图 3-11 输入打开文件时的密码

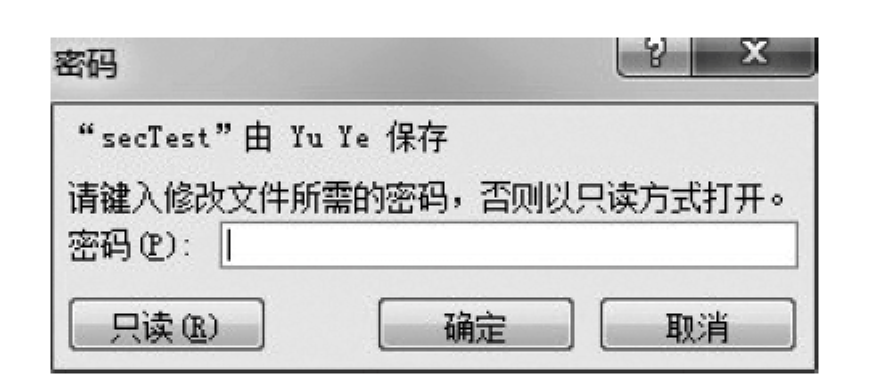


图 3-12 输入修改文件时的密码

第 4 步：修改文件。

依次输入打开文件和修改文件的密码以后就能对文件进行修改。

2. Office 加密文件的解密过程

第 1 步：下载解密软件。

到网上下载 Office Password Recovery Toolbox 并安装。

第 2 步：运行解密软件。

运行 Office Password Recovery Toolbox，选择要解密的文件(secTest. doc 文件)，如图 3-13 所示。

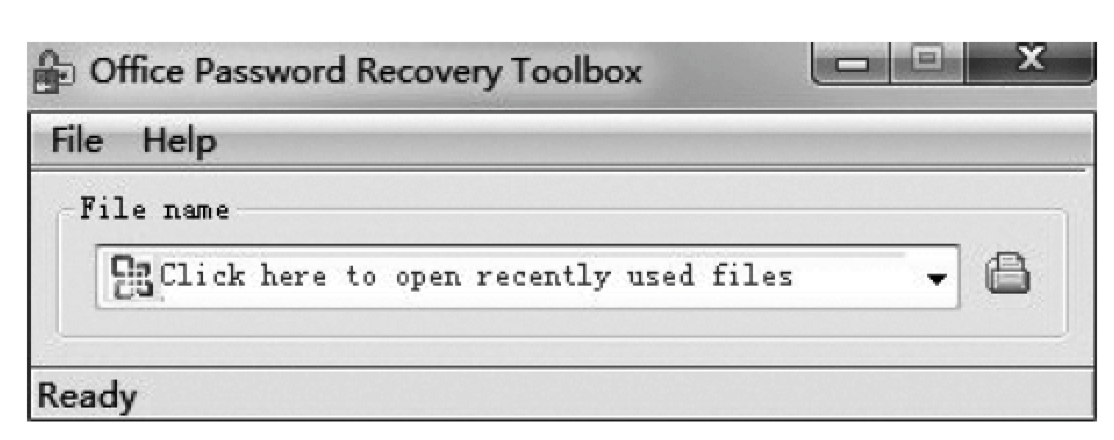


图 3-13 选择要解密的文件

第 3 步：解密文件。

（1）选择解密文件后，打开如图 3-14 所示的操作对话框，单击【Remove】按钮。

（2）出现的“信息”对话框如图 3-15 所示，提示信息大意是用该软件进行解密的前提条件是能够访问互联网，单击【OK】按钮。

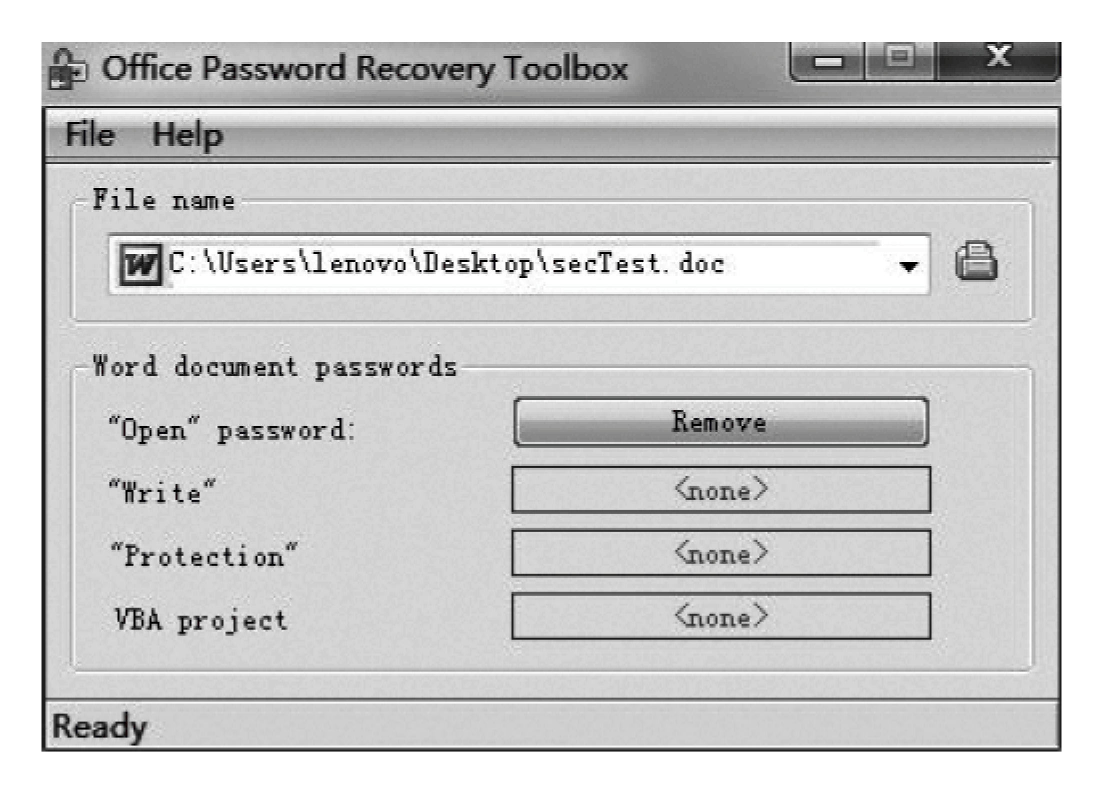


图 3-14 移除的密码

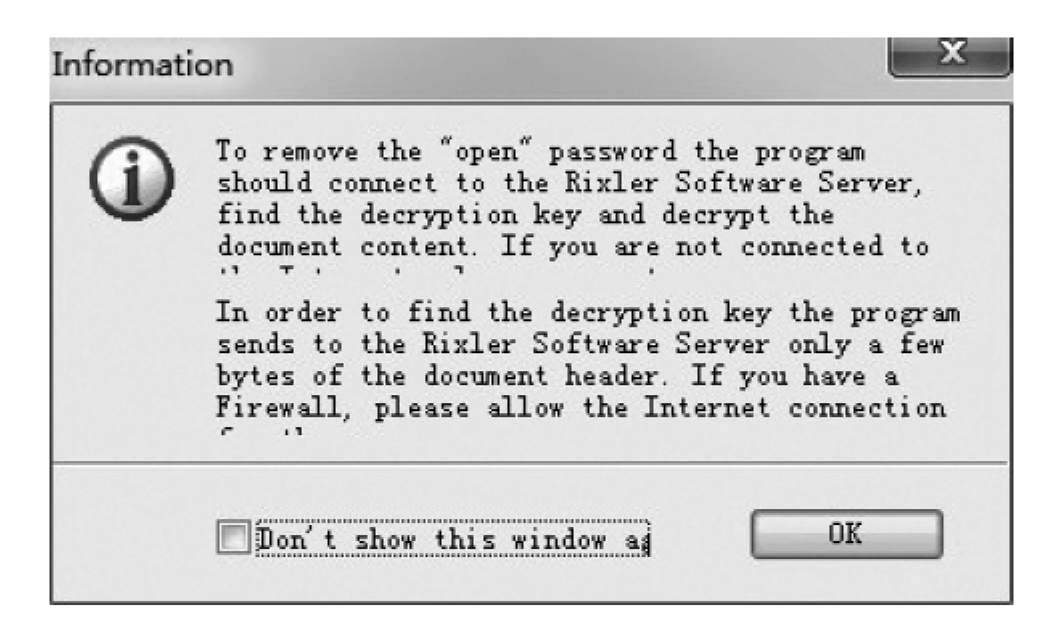


图 3-15 信息窗口

（3）过一会儿，会弹出对话框如图 3-16 所示，提示密码成功解密，单击【确定】按钮。

（4）解密成功后出现如图 3-17 所示的对话框，单击【Open document in Microsoft Word】，打开 secTest.doc 文件。

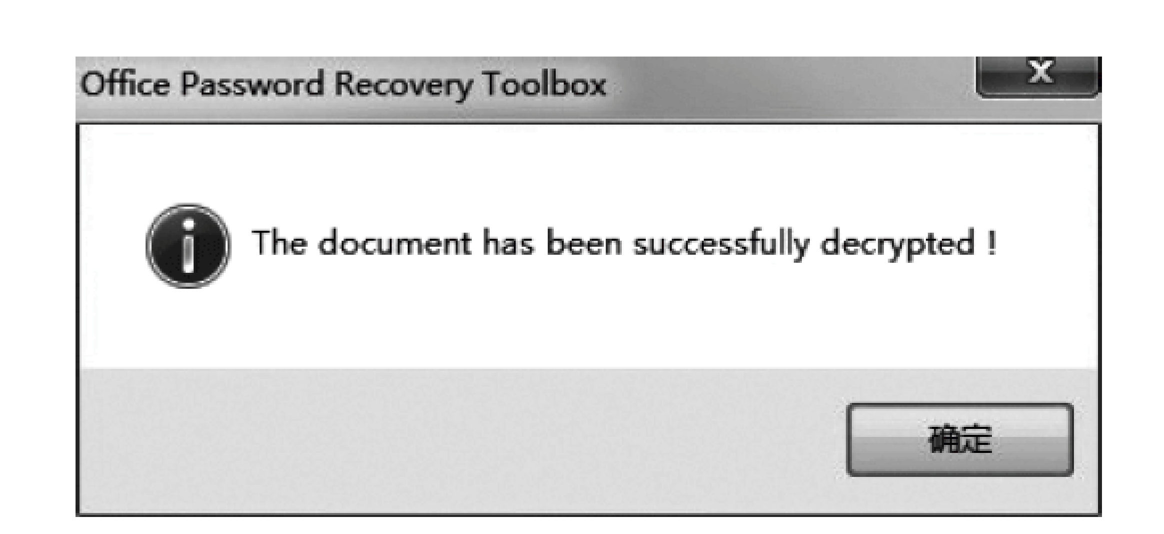


图 3-16 成功解密



图 3-17 打开 secTest.doc 文件

3.4.2 破解 Windows 用户密码

为了保证计算机的隐私性，在使用计算机的过程中通常用户都会设置 Windows 用户密码，但是如果忘记了所设置的用户密码这对用户来说也是十分棘手的一个问题。本节通过实例说明如何破解 Windows 用户登录密码。

第 1 步：创建初始文件。

（1）打开记事本，输入下面这个命令代码：

```
@Net user hack admin/add
@Net LOCALGROUP administrators hack/add
@exit
```

上面代码的意思是创建一个管理员账号,用户名:hack 密码:admin。

(2) 将这个文件保存为 TA.bat 的批处理文件。

第 2 步:制作 EXE 自解压文件。

(1) 右击 TA.bat 文件,在出现的快捷菜单中选择“添加到压缩文件…”菜单命令,如图 3-18 所示,打开“压缩文件名和参数”对话框。

(2) 在“压缩文件名和参数”对话框“常规”标签下的“压缩选项”框中勾选“创建自解压格式压缩文件”选项,如图 3-19 所示。



图 3-18 右击文件出现的菜单



图 3-19 “压缩文件名和参数”对话框

(3) 单击“高级”标签,可选择自解压格式选项,如图 3-20 所示。

(4) 设置自解压选项后,在“高级”修改界面中单击【自解压选项】按钮,将打开“高级自解压选项”对话框,如图 3-21 所示。



图 3-20 “高级”修改界面

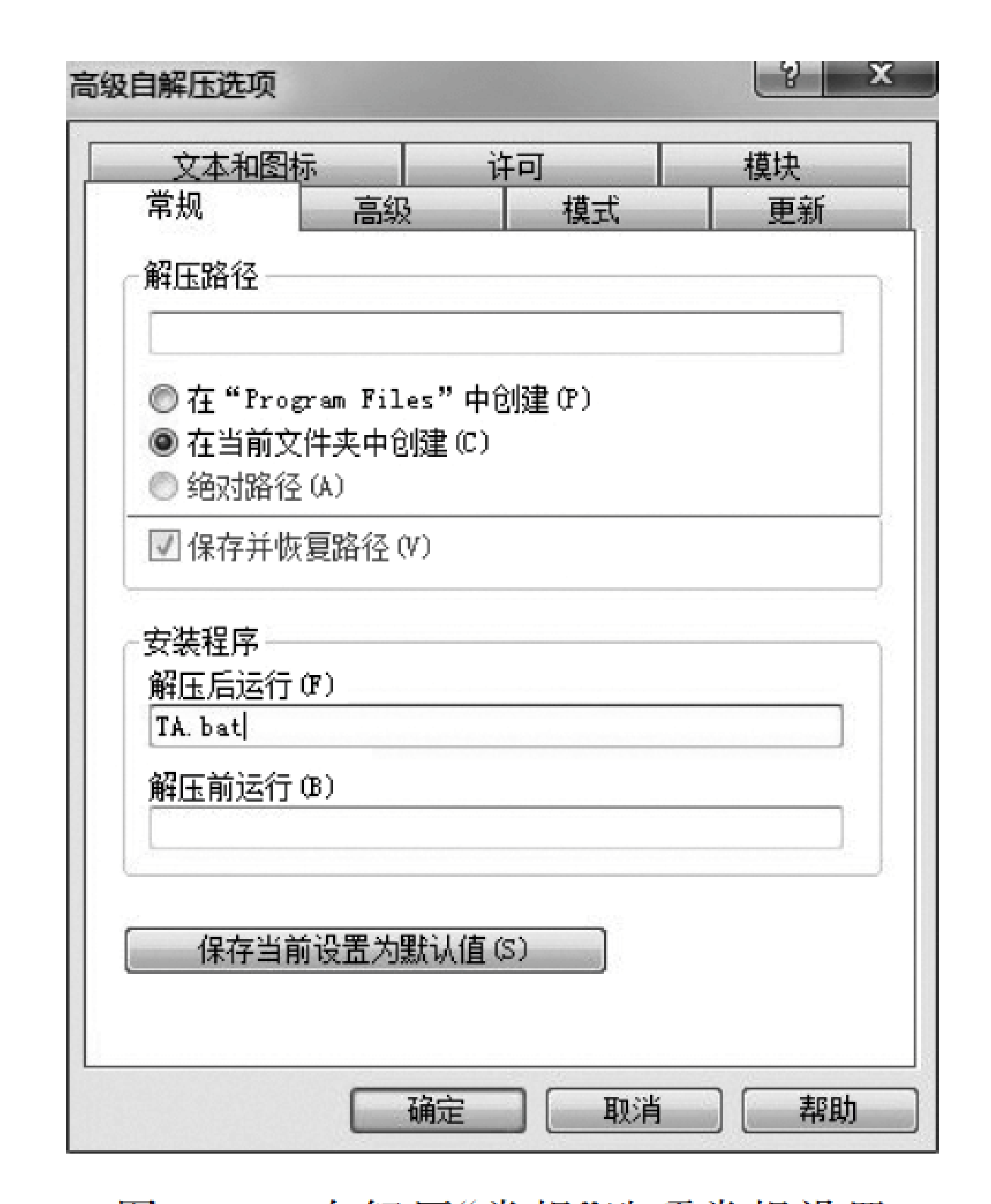


图 3-21 自解压“常规”选项常规设置

（5）在“高级自解压选项”窗口单击“常规”标签，在“解压路径”框中选择“在当前文件夹中创建”选项，在“安装程序”框的“解压后运行”栏中输入“TA.bat”。

（6）在“高级自解压选项”对话框中选择“模式”标签，在“安静模式”框中选择“全部隐藏”选项，如图 3-22 所示。



图 3-22　自解压“模式”选项模式设置

（7）单击“高级自解压选项”对话框中【确定】按钮，程序就会自动创建好 TA.exe 自解压文件，然后将创建好的 TA.exe 文件重命名为 magnify.exe（放大镜的程序名），并存到 D 盘下。

第 3 步：制作 USB 启动盘。

将 magnify.exe 这个文件复制到 U 盘上，制作 U 盘启动盘前还需上网下载 USBBOOT 软件到准备的 U 盘中。

第 4 步：破解用户密码。

（1）自解压文件替换系统自带放大镜程序。

将 U 盘插到计算机上，然后通过 BISO 设置将计算机的启动顺序设置为 USB 启动优先，进入 DOS 界面后输入 COPY D:\magnify.exe\c:\windows\system32 然后回车，可将之前制作的 magnify.exe 自解压文件替换原来系统自带的放大镜程序。

（2）重新启动计算机并拔掉 U 盘，让计算机从硬盘启动，在欢迎界面下按下 Win+U 键，此时系统就自动创建了一个用户名为 mengyang 密码为 admin 的管理员账号，并且是最高权限的账号。

（3）完成后同时按住键盘的 Ctrl+Alt+Del 组合键调出用户登录界面，输入第一步中所设置的用户名 hack 和密码 admin，这样即可登录系统。

3.5　案例讨论

服务器管理员发现一台服务器被入侵，但是不知道如何被入侵的，请专业人士辅助解决问题。简单了解了情况，服务器前有防火墙，只开放了 80、3389 端口，服务器补丁打全了。按照老习惯怀疑可能 SQL 注入，但是看 Web 日志前，习惯性地先简单看了看服务器日志，发现服务器安全日志中存在多个互联网 IP 地址从远程终端登录的记录，甚至有在夜间的。询问管理员和开发商人员，在记录的时间段内是否进行过登录，回答均没有在那个时间登录过。于是初步判断可能是密码被猜出来，攻击者直接从终端服务进行了远程登录，登录到系统上进行了操作。

做了初步判断以后，再询问管理员密码情况如何，管理员说我们密码安全性应该比较好，有字母、有特殊字符，而且 12 位长，专业人士询问具体密码，管理员给出的密码为：zaq12wsxZAQ!@WSX。乍看之下密码比较复杂，仔细查看以后发现，其实就是计算机键盘最左边的一排键，从下按到上，再从上按到下，然后按着 shift 键再重按一次。自认为

聪明的管理员，这种密码的设置方式，被攻击者知道便不再是安全的密码了。案例非常简单，但是其中牵涉到密码设置的问题，也可看出密码的设置是一个十分重要的问题。

归纳总结

1. 有哪些典型的加密算法？归纳总结不同加密算法的特点与作用。

2. 服务器密码泄露事件不胜枚举，收集归纳在其他方面与密码安全技术相关的经典案例。

3. 收集密码技术在实际中的应用案例，归纳总结密码技术的特点与作用。

思考与实践

思考题

1. 什么是密码？什么是密码学？什么是密码机制？
2. 密码技术发展过程中有哪些代表技术？
3. 密码技术有哪几种算法？特点分别是什么？
4. 现代常用密码技术应用有哪些？主要解决什么问题？
5. 你是如何理解密码技术的重要性的？

实践题

1. 根据 3.4.1 节的应用实例，设置一份加密 Word 文档并破解，记录过程中所遇到问题。尝试使用其他不同的办法破解加密 Word 文档。

2. 阅读 3.4.2 节的应用实例，了解如何破解 Windows 用户密码，并对比其他操作系统，查找相关破解密码的方法。

3. 上网搜索一种加密软件或解密软件，熟悉操作并记录使用步骤。



第4章 软件安全技术

学习目标

通过本章的学习，能够——

- 对软件安全有一个整体的认识；
- 了解软件加密技术和解密过程；
- 了解软件分析技术及相关工具；
- 熟悉几种常用的软件保护技术；
- 掌握软件加壳与脱壳工具的使用方法。

引导案例

还记得2008年曾轰动一时的微软黑屏事件吗？当时的“黑屏门”是为了配合微软公司的“全球反盗版日”活动。微软公司在2008年10月20日开始推出两个重要更新：Windows正版增值计划通知（简称“WGA通知”）和Office正版增值计划通知（简称“OGA通知”），旨在帮助用户甄别他们计算机中安装的微软Windows操作系统和Office应用软件是否是获得授权的正版软件，从而帮助那些在不知情的情况下安装和使用了盗版软件的用户免受侵害。如果使用了盗版软件，用户会不断收到正在使用盗版软件的提示。与之前推行的Windows正版增值计划有所不同，此次微软通知称未通过正版验证的Windows XP将被黑屏。

此次黑屏事件也给全球不法盗版软件分析和用户敲响了警钟。因为盗版的价格比正版软件便宜很多，所以，很多人都会在正版和盗版中选择盗版。但是，没有人意识到盗版的危害有多么严重。

每年，都会有数以万计的消费者向微软公司讲述自己如何受到盗版软件侵害的真实经历。全球各地的消费者联系微软公司，报告自己是盗版软件的受害者，并表达了对此问题的关注与忧虑。消费者举报的情况不尽相同：有人花钱购买了无法使用的产品；有人则遇到了更为严重的问题，如病毒、间谍软件、恶意软件、私人数据丢失、身份遭窃等。遭受这类打击的正是那些最脆弱的群体——个人以及中小企业，对他们来讲，时间和金钱都尤为宝贵。

2006 年，一项针对盗版软件风险的开放性调查研究在全球展开。调查人员分别在全球 17 个国家购买了盗版的微软软件，软件代码专家和法学分析师检查了这些盗版软件中的所有代码。调查结果显示，超过一半的盗版软件中含有伪代码和恶意软件，甚至无法进行安装。而这是三年前得出的调查结果，那时，全球还没有建立起对网络攻击的普遍认知。

随着现代商业软件的发展，对利润的追求使得开发商越来越看重版权。要使用软件，又不想付费，就只能盗版。因为过去的自由复制和自由交流复制已经不复存在。20 世纪 80 年代后，计算机的商业化和软件专有化席卷整个产业，免费使用软件和自由复制软件更是越来越困难，至此软件的盗版开始盛行。

软件盗版作为软件安全的主要威胁已严重影响到软件产业的发展，为了阻止盗版，很多软件公司对软件进行加密。但是，事实上，软件加密技术并不能完全阻止盗版。因为要充分保护大多数软件内容，其所需成本往往比被保护的内容本身价值还高。而相对较弱的保护方法又成了全世界黑客群体的目标。另外，加密技术不能获胜的原因还在于，要保证加密文件不流通，就要求文件的接收人拒绝与任何人分享文件。研究人员发现光靠软件加密将无法有效遏阻盗版，唯有整体安全架构才有可能解决此问题。

4.1 软件安全技术概述

本节主要介绍软件的本质和特征、软件安全保护的指导思想和软件安全面临的主要威胁，并简要介绍相应的防护技术。

4.1.1 软件及其安全的基本概念

1. 软件的定义和分类

计算机系统分为硬件系统和软件系统两部分，通常简称为硬件和软件。硬件是看得见摸得着的物理实体，如显示器、主机、打印机、键盘、鼠标、扫描仪等，它们是计算机进行工作的物质基础，软件是支配硬件进行工作的“灵魂”。软件通常包含计算机程序及其相关文档数据。根据计算机程序所起的作用，软件可分为固件、系统软件、中间件和应用软件四种类型。

(1) 固件是指一些与硬件结合较为紧密的小型软件，通常与硬件“固化”在一起。

(2) 系统软件主要是指操作系统、数据库系统和编译器软件，它们负责管理和优化计算机软硬件资源的使用。

(3) 中间件是指在计算机系统平台与计算机软件之间起桥梁作用的一组软件，如 API、ODBC、ADO 和 Web 服务器等。

(4) 应用软件是用于解决某领域的专门问题的软件，其种类繁多。

对于软件的一般要求是适用范围广、可靠性高、安全保密性强、价格适当，而对于有特殊安全保护要求的软件则一般应具备防复制、防静态分析、防动态跟踪等技术性能。

2. 软件的本质和特征

软件具有两重性，即软件具有巨大的使用价值和潜在的破坏性能量。软件的本质和特征可以描述如下：

(1) 软件是用户使用计算机的工具；

(2) 软件是将特定装置转换成逻辑装置的手段；

(3) 软件是计算机系统的一种资源；

(4) 软件是信息传输和交流的工具；

(5) 软件是知识产品，奠定了知识产业的基础，已成为现代社会的一种商品形式；

(6) 软件是人类社会的财富，是现代社会进步和发展的一种标志；

(7) 软件是具有巨大威慑力量的武器，是将人类智慧转换成破坏性力量的放大器；

(8) 软件可以存储，可以进入多种媒体；

(9) 软件可以移植，包括在相同和不相同的计算机上的软件移植；

(10) 软件可以非法入侵载体；

(11) 软件可以非法入侵计算机系统；

(12) 软件具有寄生性，可以潜伏在载体或计算机系统中，从而构成在合法操作或文件名义下的非授权；

(13) 软件具有再生性，在信息传输过程中或共享系统资源的环境下存在着非线性增长模式；

(14) 软件具有可激发性，是可接受一定(外部的或内部的)条件刺激的逻辑炸弹；

(15) 软件具有破坏性，一个人为设计的特定软件可以破坏指定的程序或数据文件，足以造成计算机系统的瘫痪；

(16) 软件具有攻击性，一个软件在运行过程中可以搜索并消灭对方的计算机程序，并取而代之。

可见软件不但是工具、手段、知识产品，同时也是一种武器，存在着潜在的不安全因素及破坏性，因此学习与掌握相应的软件安全技术是十分必要的。

3. 软件安全的含义

软件安全泛指计算机软件与数据不受自然和人为有害因素的威胁和危害，具体来说，可以理解为软件与数据不会被有意或无意地被跟踪、破坏、更改、显露、盗版、非法复制，软件系统能正常连续地运行。

4. 软件安全保护的指导思想

软件安全保护的指导思想是采用加密、反跟踪、防非法复制等技术，在软件系统或固件上产生一种信息，这种信息既是软件系统中各可执行文件在运行中必须引用的，又是各种文件复制命令或软盘复制软件所无法正确复制、无法正确安装或无法正确运行的。

4.1.2　软件安全的主要威胁

1. 软件盗版

软件盗版是指任何未经软件著作权人许可，擅自对软件进行复制、传播，或以其他方式超出许可范围传播、销售和使用的行为。

2011 年 5 月 13 日，总部设在华盛顿的国际商务软件联盟（business software alliance）发表报告说，2010 年全球软件业因盗版和非法复制遭受的损失多达 588 亿美元，与上一年相比增加了 14%。报告指出，新兴市场国家普遍存在盗版和非法复制现象，尤其以中国、俄罗斯、印度和巴西等为代表的金砖国家情况最为严重。报告中说，美国软件遭受的损失最大，为 95.2 亿美元，中国软件业遭受的损失仅次于美国，为 77.8 亿美元。目前美国只有 20%的软件是盗版软件，而在中国高达 80%的软件都是盗版软件。俄罗斯盗版软件所占的比例高达 65%。报告指出，作为全球最大的软件开发商美国微软公司遭受的损失最大。新兴市场国家 70%以上的个人计算机安装的都是盗版 Windows 系统。

2. 软件跟踪

计算机软件在开发出来以后，总有人利用各种程序调试分析工具对程序进行跟踪和逐条运行、窃取软件源码、取消防复制和加密功能，从而实现对软件的动态破译。破解软件的主要手段就是动态跟踪。

软件跟踪包括静态跟踪和动态跟踪，静态跟踪是指将可执行文件反汇编为汇编语言文件，然后分析它。而动态跟踪是利用软件工具一步一步地单步执行软件。软件跟踪本身也是软件分析的主要技术，但如若被不法分子利用，用以对软件进行非法破译，将会带来很大的安全威胁。

3. 软件漏洞

由于种种原因，软件开发商所提供的软件不可避免地存在这样或那样的缺陷，通常把软件中存在的这些缺陷称为漏洞，这些漏洞严重威胁了软件系统的安全。

在发现软件的安全漏洞以后，软件公司采取的办法多数是发布“补丁”程序，以修正软件中所出现的问题。虽然补丁的数量越来越多，但安全性却没有很大的提高，主要原因如下：

(1) 对于软件商来讲，目前还缺乏探知软件漏洞的工具，等发现漏洞之后可能危害已经发生了，“补丁”程序也只起到亡羊补牢的作用；

(2) 有些软件“补丁”是很难补上去的，即使能补上了，也不一定能补得天衣无缝；

(3) 有些用户不能及时得知软件存在漏洞和已有“补丁”的信息，即使知道了，也可能因种种原因而根本无暇安装“补丁”程序。

4.1.3　保护软件安全的技术

软件安全技术是指为保护软件与数据的安全采取的方法、手段和管理措施。本书将

介绍四种软件安全技术。

1. 软件加密技术

因为软件极易复制，所以加密是保护软件的一种必要手段。软件加密的目的就是保护软件开发者的利益，防止软件被盗版。

目前软件加密技术大致可分为两类，软加密与硬加密。软加密是用纯软件的方式来实现软件的加密，主要包括密码方式、软件的校验方式和钥匙盘方式。硬加密则是利用硬件与软件相结合来实现软件的加密，其典型产品包括加密卡、软件狗等。

2. 软件分析技术

软件分析主要作用是保障软件质量，通过分析某个软件，查找出其中包含的软件漏洞，以便开发人员修改软件，修复漏洞，提高软件质量。软件分析也应用在软件的破解、解密以及计算机病毒分析工作中。

因为软件都是机器代码程序，对于它们的分析必须使用静态或动态调试工具，分析跟踪其汇编代码。常见的软件分析技术主要包括直接阅读文档、反汇编和各种跟踪技术等。

3. 软件防盗版技术

软件防盗版技术是指通过某种技术或采取某种加密措施使得一般用户利用正常的复制命令甚至于各种复制软件都无法将软件进行完整的复制，或者是使复制得到的软件不能正常运行。它包括防止软件的非法复制和防止软件的非法安装运行两方面。

针对防盗版技术的具体实现细节可以使用纯硬件方式、纯软件方式或软硬件结合的方式，这种方式即采用了对应的加密技术原理。从软件的发行载体(软磁盘、光盘以及计算机网络)入手，软件防盗版技术又包括磁盘防复制技术和光盘防复制技术。

4.2 软件加密技术

软件加密是软件商为了保护软件产品而采取的一种保护方式。软件加密主要有两种形式：(1)不依赖硬件的加密(软加密)方案；(2)依赖特定硬件的加密(硬加密)方案。本节将介绍这两种加密方式涉及的软件加密技术。

4.2.1 软件硬加密

硬加密的原理是将加密信息固化在某个硬件电路中，然后将它作为一个软件的附加设备一起交给用户。当用户运行该软件的时候，将该固化的电路设备接到计算机连接端口，软件将根据是否检测到对应的“密钥”来决定运行该软件或者屏蔽某些功能。这类硬加密常见的有软盘加密、加密狗、软件锁等。

1. 软盘加密

钥匙盘的方式是最常见的软盘加密方式。所谓钥匙盘方式就是通过 BIOS 的 INT13

中断对软盘格式化一些特殊的磁道，有的还在特殊磁道里写入一定的信息，软件在运行时要校验这些信息。这种软盘就好像一把“钥匙”一样，所以被人习惯称为钥匙盘。如KV3000等杀毒盘和早期的计算机等级考试安装盘就采用了这种加密方式。它们的主要特点是在软磁盘的特殊位置做标记，在软件运行中计算机要读取这些特殊标记，以验证软件的合法性。由于记录这种特殊标记的位置不能被平常的复制命令或复制软件所读取，所以，钥匙盘类的软件不能被轻易复制，这样，加在软件中的“锁”就变得安全有效了。

2. 加密狗

加密狗是插在计算机并行口上的软硬件结合的软件硬加密产品，包括加密代码程序和“密钥”(亦称加密盒)两部分。“密钥”中存放了“密码”，加密代码程序检查“密钥”是否存在，是否正确，在无误的情况下，去执行正常功能的应用程序。在稍后章节中将会对加密狗的原理和应用做详细的介绍。

3. BIOS 序列号

在计算机的升级之中，主板是面临淘汰的可能性最小的硬件，因此，主板序列号是主板唯一的标志，可以被运用到软件的加密中。主板序列号其实就是 BIOS 序列号，因为每台计算机的主板都有唯一的标志——BIOS 序列号，所以可以将这个序列号作为软件的认证信息。

4.2.2 软件软加密

软加密是一种低成本的加密方式。它的特点是不需要有辅助的硬件存在，直接在软件中进行加密或设立密码。相关的方法有序列号法、密码表加密法和许可证法。

1. 序列号法

序列号法是用户在购买正版软件的时候供应商提供给他们正确的密码，从而使他们顺利安装和使用购买的软件的方法。但是，由于计算机软件的易复制性，盗版软件只需复制软件及安装序列号，一样能够完成安装并顺利运行，在软件功能上没有任何缺损。因此，这种类型的“钥匙”其实成了一种象征性的摆设，加密强度不够。

2. 密码表加密法

密码表加密法是程序在运行时提出一些提示问题，用户需要按提示问题回答，如果回答答案错误则程序停止运行。正常情况下，只有输入正确的答案，软件才认为是合法使用者。这种加密方法运行简单，使用广泛。但是，因为密码表的特征字串很容易被复制，盗版者可以把整个密码表输入到计算机中存成一个文件，同盗版的软件一同公布出来，所以很容易被盗版者利用。

3. 许可证法

从某种角度上说，这种方式是序列号加密的一个变种。用户从网上下载的或购买的

软件并不能直接使用,软件在安装时或运行时会对计算机进行一番检测,并根据检测结果生成一个计算机的特定指纹,这个指纹可以是一个小文件,也可以是一串谁也看不懂的数,需要把这个指纹数据通过 Internet、E-mail、电话、传真等方式发送到开发商那里,开发商再根据这个指纹给用户一个注册码或注册文件,一般称其为许可证,用户得到包含注册码或注册文件的许可证后,按软件要求的步骤在计算机上完成注册后方能使用。

带有许可证的软件交易可以完全通过网络来进行,用户购买的软件将限制只能在自己的计算机上运行,换到其他的计算机上,其注册码或注册文件可能不再有效,用户更换某些硬件设备也可能造成注册码的失效,而且用户得到软件后在完成注册工作前会有一段时间无法使用软件。

许可证法对于软件开发商来说服务与管理的工作量无疑是非常巨大的。

4.3 软件分析技术

软件逆向工程(software reverse engineering)又称软件反向工程,是指通过可运行的程序,运用解密、反汇编、系统分析等手段,对软件的结构、流程、算法、代码等进行逆向分析和拆解,从而推导出软件产品的源代码、设计原理、结构、算法、处理过程、运行方法等。通常人们把对软件进行反向分析的整个过程统称为软件逆向工程,把在这个过程中所采用的技术都统称为软件逆向分析技术。

随着软件逆向分析技术的发展,软件安全受到的威胁也越来越大。通过分析技术,破解者可以获取二进制程序的反汇编代码,进行静态的程序控制流程分析和动态的程序跟踪调试,可以做到挖掘程序漏洞、获取关键代码的算法、绕过身份验证、做出注册机、去除版权信息、篡改程序功能等。

软件保护与逆向分析是矛与盾的关系,二者相互促进发展。当今的软件保护技术大部分都是从防止软件被逆向分析入手的,实际上,如果给逆向工程人员足够的资源,没有一种保护技术是不能被破解的。为了更好地保护软件,有必要首先了解软件逆向分析的主要技术即静态分析技术与动态分析技术,同时软件分析技术也是软件开发人员需要掌握的工具,通过分析技术可以弥补漏洞,提高软件的质量。

本节主要介绍软件逆向分析的静态分析技术、动态分析技术与漏洞挖掘技术。

4.3.1 静态分析技术

静态分析就是对反汇编得到的程序清单进行分析,从提示信息入手,了解该程序的流程与模块完成的功能。如果对静态反汇编出来的程序清单进行仔细阅读,就可以了解该软件的编程思路,实现对其进行解密。

软件静态分析技术的本质是对软件进行反汇编处理,然后分析汇编语句列表,从中摸索出软件运行的机制,试图破解软件的保护机制。

1. 静态分析破解步骤

对软件采用静态分析破解一般有以下几个步骤:

(1) 侦察软件的文件类型,确定软件的运行文件是否经过加壳(软件加密或压缩)处理;

(2) 如果软件被加壳,则需要使用工具进行脱壳处理;

(3) 运行待破解的目标软件,一般会要求输入用户名、注册码或序列号等,任意输入一个,软件将会给出错误提示,把该提示记录下来;

(4) 备份目标文件,使用反汇编工具如 W32Dasm 或 IDA Pro 等对软件进行反汇编处理;

(5) 在反汇编后的代码里找到前面记录的出错提示字符串;

(6) 在该字符串附近仔细分析各种跳转指令和比较指令,如 CMP,TEST 指令等,试图找出判断注册码或序列号正误的分支,记下该指令在文件中的偏移地址;

(7) 使用编辑工具如 WinHiex 或 Ultraedit 打开目标文件,按照前面获得的偏移地址,在文件中找到对应的指令代码,修改后存盘,破解完毕。

2. 静态分析使用的基本工具

下面介绍几种静态分析破解过程中所用到的基本工具。

(1) 文件类型分析工具。

对软件进行静态分析时首先要了解和分析程序的类型,了解程序是用什么语言编写的,或用什么编译器编译的,程序是否有加壳保护。常用的文件类型分析工具有 Language 2000、PEiD、File Scanner、FileInfo 等。

Language 2000 是文件类型检测工具,可用检测出文件的最终编译程序或文件加壳、加密类型。此版本共支持 45 种编译器和 42 种加壳、加密类型。

PEiD 是一款著名的查壳工具,其功能强大,几乎可以侦测出所有的壳,其数量已超过 470 种 PE 文档的加壳类型和签名。

(2) 静态反汇编工具。

常用的静态反汇编工具有 W32Dasm、IDA Pro 等。

W32Dasm 可以方便地反汇编程序,它能静态分析程序流程,也可动态分析程序,在其新版本中,还加强了对中文字符串的提取,这增加了对国产共享软件的威胁。

IDA 是一个极好的反汇编工具,同 W32Dasm 有很多相同的功能。例如,它可以加速到达指定的代码位置。可以看到跳到指定位置的 JMP 命令的位置,可以查看参考字符串,可以保存静态汇编等。IDA Pro 比 W32Dasm 有更多的选项和更先进的技术,可以更好地进行反汇编和深层的分析。

(3) 可执行文件编辑修改工具。

在对文件进行分析的时候,还可以使用某些专门的工具软件来对这些可执行文件进行编辑修改,如前面所讲的 W32Dasm 和 IDA Pro 都是适合分析文件的工具。如果要对文件进行编辑修改,则需要专门的十六进制工具。这方面常用的工具有 Hiew、HexWorkshop、WinHiex、Ultraedit 等。Hiew 是一个十六进制工具,它除了普通的十六进制外,还可方便快捷地用汇编指令修改程序。

4.3.2 动态分析技术

用静态分析法可以了解编写程序的思路，但不能真正地了解软件编写的整个细节和执行过程，在对软件静态分析无效的情况下可以对程序进行动态分析。

动态分析就是通过调试程序、设置断点、控制被调试程序的执行过程来发现问题。

1. 软件动态跟踪分析步骤

对软件动态跟踪分析时可以分两步进行。

(1) 对软件进行粗跟踪。

所谓粗跟踪，即在跟踪时，大块大块地跟踪，也就是说，每次遇到调用 CALL 指令、重复操作指令 REP、循环操作 LOOP 指令以及中断调用 INT 指令等，一般不用跟踪进去，而是根据执行结果分析该段程序功能。

(2) 对关键部分进行细跟踪。

在获取软件中关键模块后，便可以获取软件中我们关心的模块或程序段，这样就可以针对性地对该模块进行具体而详细的跟踪分析。在一般情况下，对关键代码的跟踪可能要反复进行若干次才能读懂该程序，每次要把比较关键的中间结果或指令地址记录下来，这样会对下一次分析有很大的帮助。

2. 动态分析调试器模式

动态分析技术使用的调试器可分为用户模式和内核模式两种类型。

(1) 用户模式。

用户模式调试器工作在 Win32 的保护机制 Ring 3 级(用户级)上，如 Visual C ++等编译器自带的调试器就是用户级的。

(2) 内核模式。

内核模式调试器是指能调试操作系统内核的调试器，它们处于 CPU 和操作系统之间，工作在 Win32 的保护机制 Ring 0 级(特权级)上，如著名的 Soft-ICE 调试器。常用的动态分析工具有 Soft-ICE 和 TRW2000 等。Soft-ICE 是目前公认的最好的跟踪调试工具。使用 Soft-ICE 可以很容易地跟踪一个软件或监视一个软件产生的错误，并进行除错。TRW2000 完全兼容 Soft-ICE 的各条指令，并且专门针对软件破解进行了优化，在 Windows 9× 下跟踪调试功能更强，可以设置各种断点，并且断点种类更多。它可以像一些脱壳工具一样完成对加密外壳的去除，自动生成 EXE 文件。

软件分析是一种比较复杂和艰苦的工作。上面只是提供了一些基本的分析方法，要积累软件分析的经验，需要在实践中不断探索和总结。

4.3.3 漏洞挖掘技术

软件漏洞也称为脆弱性(vulnerability)，它是计算机软件在程序的设计和实现过程中由于各种原因有意或无意中产生的不足与缺陷。目前主要的软件漏洞有拒绝服务、内存/交换区漏洞、符号连接、竞争条件、缓冲区溢出、格式化字串、rhost，xhost 等。

1. 软件漏洞攻击

非法用户利用软件漏洞，对计算机进行的非授权操作以及所有危害计算机系统安全的行为，都被视为软件漏洞攻击行为。软件漏洞攻击行为不仅可以使攻击者获得访问权限的提升，甚至能够执行任意代码。由此可见。软件漏洞对计算机系统安全的威胁是十分巨大的。

漏洞攻击技术主要包括漏洞挖掘技术和漏洞利用技术。漏洞挖掘技术是发现漏洞的主要手段。漏洞利用技术则是通过研究已发掘漏洞，开发出相应的利用代码，生成具有攻击性的文件或程序，该文件或程序在被浏览或运行后可以触发软件漏洞，从而达到攻击的目的。

2. 软件漏洞挖掘

漏洞挖掘是漏洞攻击的重要环节，只有先挖掘出漏洞，才能够通过漏洞利用技术进行漏洞攻击。软件安全漏洞发掘可以分为对已知漏洞的检测和对未知漏洞的挖掘。已知漏洞的检测主要是通过安全扫描技术，发现系统是否存在已公布的安全漏洞。而未知漏洞挖掘的目的在于发现软件系统中可能存在但尚未发现的漏洞。现有的未知漏洞挖掘技术从操作的自动化程度角度，可分为手工分析和自动/半自动化分析；从软件的运行态角度，可分为静态检测和动态检测；从软件代码的开放性角度，可分为白盒测试、黑盒测试和灰盒测试。

3. 基于逆向分析的漏洞挖掘技术

下面结合本节逆向分析技术的内容介绍基于逆向分析的漏洞挖掘技术。

基于逆向分析的软件漏洞挖掘技术是将要分析的二进制代码首先反汇编，得到汇编代码；然后对汇编代码进行切片。即对某些上下文关联密切、有意义的代码进行汇聚，降低其复杂性；最后通过分析功能模块来判断是否存在漏洞。

按照是否采用反汇编和反编译得到其高级语言表述的代码，可以将逆向工程的方法分为白箱分析法和黑箱分析法。

白箱分析法主要指对源代码进行分析和理解。对于所需分析的二进制代码，采用反汇编、反编译的方法，得到其高级语言形式的源代码，并进一步分析此源代码。这种方法可以认为是白箱分析。如果有优秀的反编译工具的支持，白箱测试对于发现软件中设计错误和执行错误是非常有效的。然而白箱测试也有不足之处，就是编译后产生的代码和其真正的源代码可能会存在差异，因此可能会误报实际上不存在的漏洞。

黑箱分析法就是利用各种输入对程序进行探测，并对程序运行的结果进行分析。这种分析方法仅需要有运行的程序而不需要分析任何形式的源代码。其测试条件是可运行的程序、能接受输入以及可以观察到结果。如果测试者能给运行的程序提供输入，并可以观察输出结果，就可以进行黑箱测试。在黑箱测试时，可以尽量给程序提供各种恶意输入向量，如果用某个特定的测试向量测试程序时程序出现异常，就预示着可能发现了该程序的一个漏洞。相对于白箱测试，黑箱测试在理解代码逻辑和程序行为等方面不是那么有

效，而且黑箱测试需要软件分析者具有更多的经验。不过黑箱测试不需要反汇编、反编译等工具的支持，更容易实现。

下面介绍两种比较典型的漏洞挖掘技术，其中利用静态分析工具自动分析属于白箱分析法，代码覆盖测试属于黑箱分析法。

（1）利用静态分析工具自动分析。

采用反汇编工具所提供的脚本语言对漏洞进行自动挖掘也是一种有效的漏洞挖掘技术。可采用的工具包括 IDA Pro、REC 反编译工具、W32Dasm 等。其中 IDA Pro 提供了一个开放式的架构。包括 API 接口及 SDK，用户可以通过编写特定目的的自动化的脚本对反汇编数据库内的内容进行处理。以缓冲区溢出为例来说明如何编写脚本进行自动分析。很多软件程序会在环境变量处理中出现缓冲区溢出，最常见的是 getenv()调用后很快就对返回结果进行 strcpy()/sprinff()操作，而在此之前没有调用 strlen()判断返回值的长度是否小于缓冲区大小，从而导致安全问题。可以根据这个特性编写 IDC 脚本对目标实施几步搜索：

① 如果找到 getenv()调用就记录调用处的位置；

② 在 getenv()调用的后面一段范围内搜索 strcpy()/sprinff()调用，如果找到则记录调用处位置；

③ 在 getenv()调用和 strcpy()/sprinff()调用之间查找是否出现过 strlen()调用，如果没有出现过则报警，在 IDA 的信息栏中显示 getenv()调用的地址。

根据以上算法编写相应的 IDC 脚本，然后在对可执行码反汇编结束后执行该脚本。如果被测试的可执行码中有函数与以上算法所描述的规则相匹配，就能够很快地定位漏洞。

（2）代码覆盖测试。

代码覆盖测试是软件测试和评估中的重要方法，它能评估软件测试完成程度，包括语句覆盖、判定覆盖、条件覆盖、条件组合覆盖等内容。同样利用代码覆盖工具，分析者可以观察程序执行情况，并判断代码执行的是哪条路径。不少工具都可以进行代码覆盖分析。代码覆盖分析可以在分析者分析软件情况时告诉他还有多少目标评估工作没有完成。代码覆盖测试不需要目标软件的源代码，一些代码覆盖工具能附加到进程之上，并实时收集评估信息。

覆盖测试技术可以和输入追踪技术结合使用。例如，对 WSARecvFrom0 的调用，使用外部输入追踪，可以估计访问的代码路径。当程序接受了用户的数据输入，根据具体的条件会执行不同的代码分支，这些逻辑是通过机器代码的条件分支指令来实现的。例如 x86 机器代码中的 JNZ 和 JE 等指令都是用来实现条件分支的。代码覆盖工具可以检测什么时候会执行分支，并可以画出连续执行的一段机器代码的执行图，有助于判断在分析中还有哪些路径没有走过。

4. 软件漏洞利用

不是所有软件漏洞都能够被利用，能被利用的漏洞也不一定值得利用。一般而言，危险等级高的，特别是漏洞描述中提到了“任意代码执行”的漏洞，利用价值最高，危害程度也就越大。这类漏洞触发之后，通常会造成溢出，从而获得代码执行的权。漏洞利用技术

主要就是通过构造畸形数据造成溢出，进而执行恶意代码。

常见的利用软件缺陷对应用软件系统发起攻击的技术包括缓冲区溢出攻击、堆溢出攻击、栈溢出攻击、格式化串漏洞利用等，在上述漏洞利用成功后，往往借助于 shellcode 跳转或者执行攻击者的恶意程序。

(1) 缓冲区溢出利用。

如果应用软件存在缓冲区溢出漏洞，可利用此漏洞实施对软件系统的攻击。缓冲区是内存中存放数据的地方。在程序试图将数据放到计算机内存中的某一个位置的时候，如果没有足够的空间就会发生缓冲区溢出。攻击者写一个超过缓冲区长度的字符串，程序读取该段字符串，并将其植入到缓冲区，由于该字符串长度超过常规的长度，这时可能会出现两个结果：一个是过长的字符串覆盖了相邻的存储单元，导致程序出错，严重的可导致系统崩溃；另一个是利用这种漏洞可以执行任意命令，从而达到攻击目的。

程序运行时，将数据保存在内存的缓冲区中，为了不占用太多的内存，一个由动态分配变量的程序在程序运行时才决定给它们分配多少内存空间。如果在动态分配缓存区中放入超长的数据，就会发生溢出，这时程序就会因为异常而返回；如果攻击者用自己攻击代码的地址覆盖返回地址，这是通过 eip 改变返回地址，可以让程序转向攻击者的程序段；如果在攻击者编写的 shellcode 中集成了文件的上传和下载等功能，获取到 root 权限，那么就相当于完全控制了被攻击方，也就达到了攻击者的目的。

(2) 栈溢出利用。

程序每调用一个函数，就会在堆栈中申请一定的空间，把这个空间称为函数栈。而随着函数调用程序的增加，函数栈一块块地从高端内存向低端内存地址方向延伸；反之，随着进程中函数调用层次的减少，即各函数调用的返回，函数栈会一块块地被遗弃而向内存的高址方向回缩。各函数栈的大小随着函数性质的不同而不等，由函数的布局变量的数目决定。进程对内存的动态申请是发生在堆里的，也就是说，随着系统动态分配给进程的内存数量的增加，Heap 有可能向高地址或低地址延伸，依赖于不同 CPU 的实现，但一般来说是，向内存的高地址方向增长的。

当发生函数调用时，先将函数的参数压入栈中，然后将函数的返回地址压入栈中，这里的返回地址通常是 Call 的下一条指令的地址。例如，定义 buffer 时程序可分配 24B 的空间，在 strcpy 执行时向 buffer 里复制字符串时并未检查长度，如果向 buffer 里复制的字符串如果超过 24B，就会产生溢出；如果向 buffer 里复制字符串的长度足够长，把返回地址覆盖后程序就会出错。一般会报段错误或者非法指令，如果返回地址无法访问，则产生段错误，如果不可执行，则视为非法指令。

(3) 堆溢出利用。

堆内存由分配很多的大块内存区组成，每一块都含有描述内存块大小和其他一些细节信息的头部数据。如果堆缓冲区遭受了溢出，攻击者能重写相应堆的下一块存储区，包括头部。如果重写堆内存区中下一个堆的头部信息，则在内存中可以写进任意数据。然而，不同目标软件各自特点不同，堆溢出攻击实施较为困难。

(4) 格式化串漏洞利用。

格式化串，就是在 * printf()系列函数中按照一定格式对数据进行输出，可以输出到

标准输出,即 printf(),也可以输出到文件句柄、字符串等,对应的函数有 fprintf 、sprintf、snprintf、vprintf、vfprintf、vsprintf、vsnprintf 等,能被黑客利用的地方也就出在这一系列的 * printf()函数中。

(5) shellcode 技术。

缓冲区溢出成功后,攻击者如希望控制目标计算机,必须用 shellcode 实现各种功能。shellcode 是一堆机器指令集,基于 x86 平台的汇编指令实现,用于溢出后改变系统的正常流程,转而执行 shellcode 代码从而完成对目标计算机的控制。

5. 软件漏洞攻击的防范

防范软件漏洞攻击需要软件开发商、政府、用户三方面通力配合,才能够有效减少软件漏洞所带来的危害。

软件开发商应当对所开发的软件负责,采用更加严格的软件安全测试技术,在生产环节就有效降低发掘软件漏洞的可能性。软件开发商还应该具备及时提供修补软件漏洞补丁的能力。虽然微软公司的产品漏洞很多,但是相对于其他软件要安全得多。

政府作为信息产业的管理者,应当建立软件漏洞检测与公告机制。通过软件漏洞检测,尽可能主动挖掘软件的潜在漏洞,并通知软件生产商发布升级补丁修补漏洞或者推出新版本。软件漏洞公告可以建立在类似于 CVE 等组织的漏洞公告网站。在发布漏洞信息的同时,还应建立软件漏洞信息数据库,方便软件漏洞的分类与管理。同时,软件漏洞公告还有利于杀毒软件商升级病毒库,以查杀漏洞利用文件。在我国,中国信息安全测评中心(CNITSEC)也建立了漏洞数据库 CNNVD,并通过其网站和刊物发布漏洞公告。

用户作为软件的使用者,是软件漏洞攻击的最直接目标。用户应及时进行软件升级,以修补软件中存在的漏洞。但是多数用户的安全意识不高,认为软件的自动更新功能很不必要,直接将该功能关闭,同时又不关注软件漏洞信息的发布,不进行手动更新,这样的用户最容易成为软件漏洞攻击的受害者。

4.4 软件加壳与脱壳技术

针对软件逆向分析的威胁,出现了用来防止软件被逆向分析的软件加壳技术,它可以防止软件信息被披露、篡改及盗版。

恶意软件和病毒为了避免被杀毒软件分析和识别也会使用加壳技术,只是动机不良,为了保护合法软件的安全,在掌握软件加壳方法的同时有必要学习软件脱壳的技巧,来识别恶意软件和病毒。

本节主要介绍软件加壳的原理、软件加壳与脱壳工具。

4.4.1 软件加壳的原理

1. "壳"的定义

在自然界中,植物用壳来保护种子,动物用壳来保护身体等。根据其原理,在一些计

算机软件里也设计了一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。由于这段程序和自然界的壳有相似的功能，基于命名的规则，这样的程序称为“壳(shell)”。

2. “壳”的作用

通俗而言，壳的作用就是对待保护的程序进行压缩或加密。在加壳后的程序里，壳先于原程序拿到运行的控制权，对原程序进行解压或解密之后，再运行原程序，这样就可以有效防止程序被反编译或非法修改；从本质上讲，壳是一种专门针对 EXE、COM、DLL 等文件进行的压缩或加密的工具，使原程序文件代码失去本来的面目，达到程序不被反编译和非法修改的目的，软件加壳的原理如图 4-1 所示。

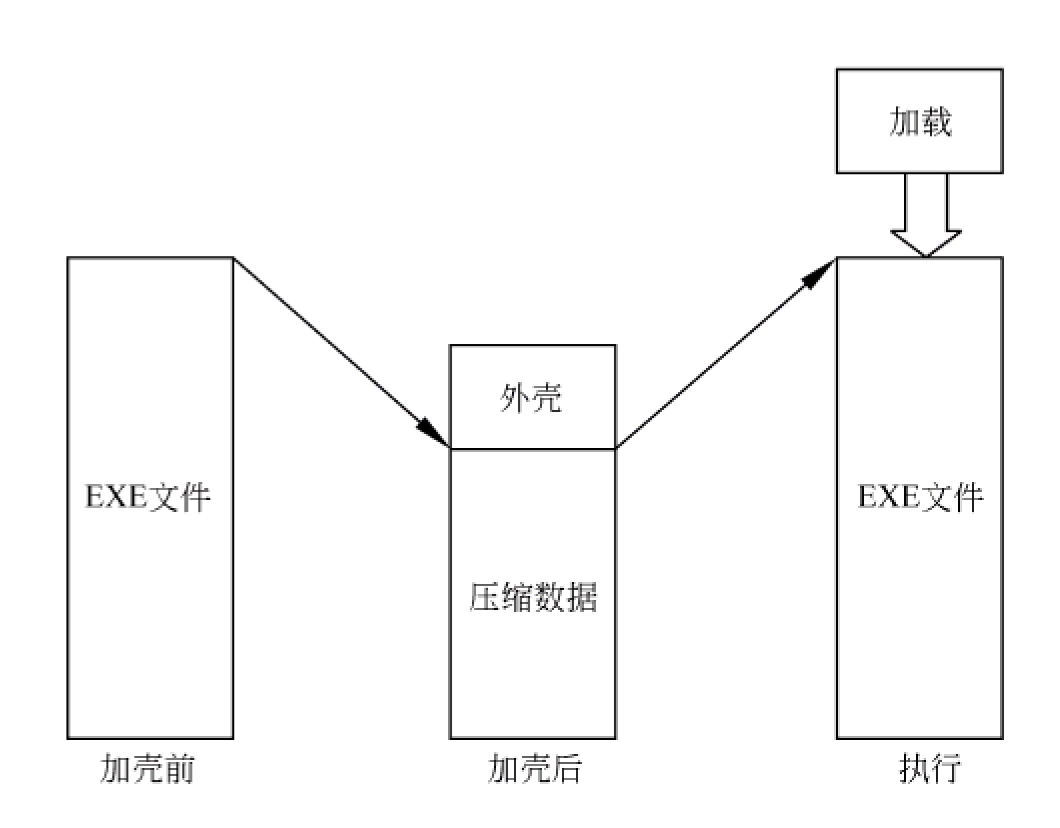


图 4-1　软件加壳的原理示意图

3. “壳”的加载过程

“壳”的加载过程由以下步骤组成：

(1) 解密程序“块”的数据。

“壳”在加密时候，对程序的“块”做了加密，PE 文件的“块”表示了程序的代码段、数据段、资源段等，在加载壳程序后，壳首先便会对这些“块”进行解密。

PE 是 Portable Execute 的简写，中文含义为可移植的执行体，常见的 EXE、DLL、OCX、SYS、COM 都是 PE 文件，PE 文件是微软 Windows 操作系统上的程序文件，可能被间接执行，如 DLL，也可以直接执行，如 EXE。

(2) 获取“壳”的 API 地址。

“壳”在解密的过程中，难免要用到一些 API 函数，而“壳”并非调用了原程序的 IAT 表(import address table，导入地址表)内相关的 API 函数，而是由自身模拟 PE 文件的组装方式，建立了属于自己的 IAT 表。

(3) “壳”软件重定位。

程序运行的时候，系统需要将程序加载到系统指定的内存中，这个初始内存地址称为基地址(ImageBase)。可以在 PE 文件头中预先申明需要加载在内存中的哪个地方，但是系统不一定能够保证程序运行时就一定能够加载在基地址。对于 EXE 扩展名的程序文件来说，Windows 系统会尽量满足。

(4) 还原 IAT 表。

IAT 表的重要性在加密与解密中是非常重要的。对于压缩型的“壳”软件来说，可能通过解密原程序就完成了对 IAT 表的修复。而对于加密型的“壳”软件来说，并不一定就会完全还原原程序的 IAT 表，可能会采用一些特殊处理方式。

(5) 跳转到程序原入口点。

无论“壳”如何操作，到最后还是要把程序控制权限交给原程序的，通常称之为 OEP(original entry point，程序原入口点)。

4.4.2 软件加壳工具

按照软件加壳的目的和方法,壳可分为压缩壳(packers)与保护壳(protectors)两类。压缩壳的主要目的是为了减小程序体积,如 ASPack、UPX 和 PECompact 等。

压缩壳的实现相对简单,在传统的此类壳中,并没有过多地引入反跟踪、反破解技术,因此其脱壳相对容易,针对不同的压缩壳,一般都有相应的脱壳机。

保护壳更加注重加壳软件的安全性,因此用上了各种反调试、反分析等先进技术,保证程序不被调试、脱壳,其加壳后的体积大小不是其考虑的主要因素,如 ASProtect、Armadillo、Themida 等。

随着加壳技术的发展,这两类软件之间的界线越来越模糊,很多加壳软件除具有较强的压缩性能,同时也有了较强的保护性能。

下面介绍几种最常用的加壳工具。

1. ASPack

ASPack 是专门针对 Win32 下 PE 文件的压缩软件,其压缩和保护性能非常好,其运行界面如图 4-2 所示,从中不难看出其使用方便、操作简单的特点。通常意义上的压缩工具,是将计算机中的资料或文档进行压缩,主要用来缩小储存空间或将多个文件压缩成一个文件,这样有利于文件的传播和存储,但是经通常意义上的压缩工具压缩后的文件就不能运行,如果想运行必须先解压缩。另外当系统中无压缩软件时,压缩包将无法解开。ASPack 是专门对 Win32 可执行程序进行压缩的工具,压缩后程序能正常运行,不会受到任何影响,即使已经将 ASPack 从系统中删除,曾经压缩过的文件仍可正常使用,ASPack 内置多种语言,包括简体中文。

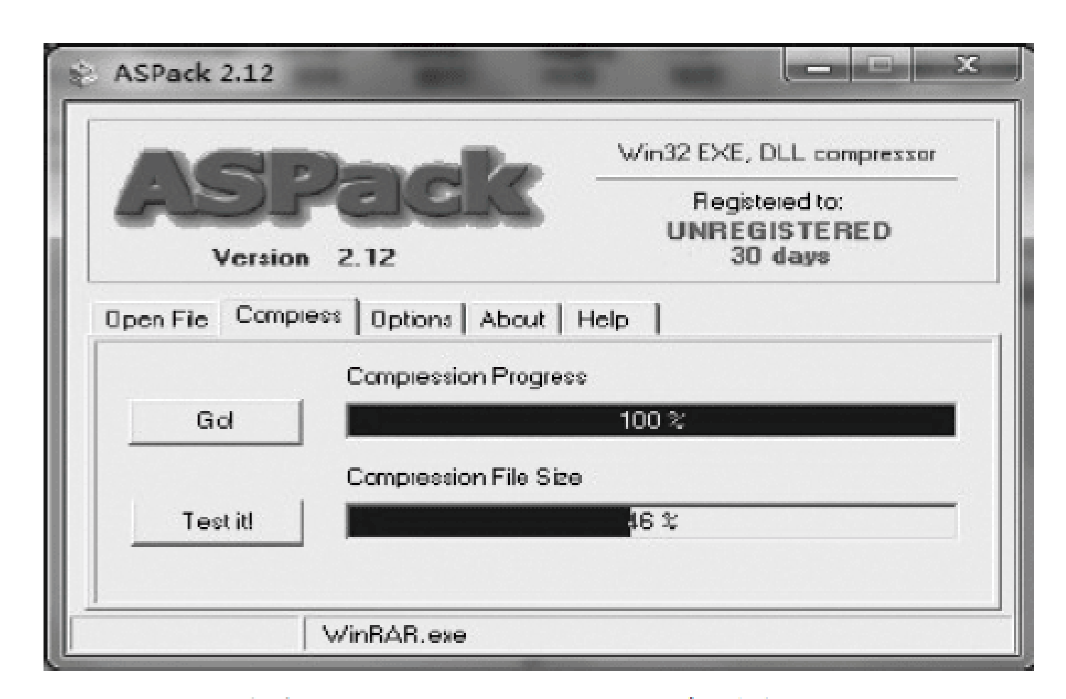


图 4-2 ASPack 运行界面

2. UPX

UPX(ultimate packer for executables)是一款先进的可执行程序文件压缩器,压缩过的可执行文件体积缩小 50%~70%,这样减少了磁盘占用空间、网络上传下载的时间和其他分布以及存储费用。通过 UPX 压缩过的程序和程序库完全没有功能损失和压缩之前一样可正常地运行,对于支持的大多数格式没有运行时间或内存的不利后果。UPX 有很多版本,支持许多不同的可执行文件格式,包含 Windows 95/98/ME/NT/2000/XP/CE 程序和动态链接库、DOS 程序、Linux 可执行文件。其运行程序界面如图 4-3 所示。

3. ASProtect

ASProtect 是一款具有高效保护性、功能非常完善的加壳工具,该软件具有压缩和强劲的保护功能,加壳后的软件不内置解压缩,壳保护机制较好,它能够在对软件加壳的同时进行各种保护,如反调试、自校验及密钥加密保护等,还有多种使用限制措施,如使用天

数限制、次数限制及对应的注册提示信息，另外，该软件还具有密钥生成功能，其运行界面如图 4-4 所示。

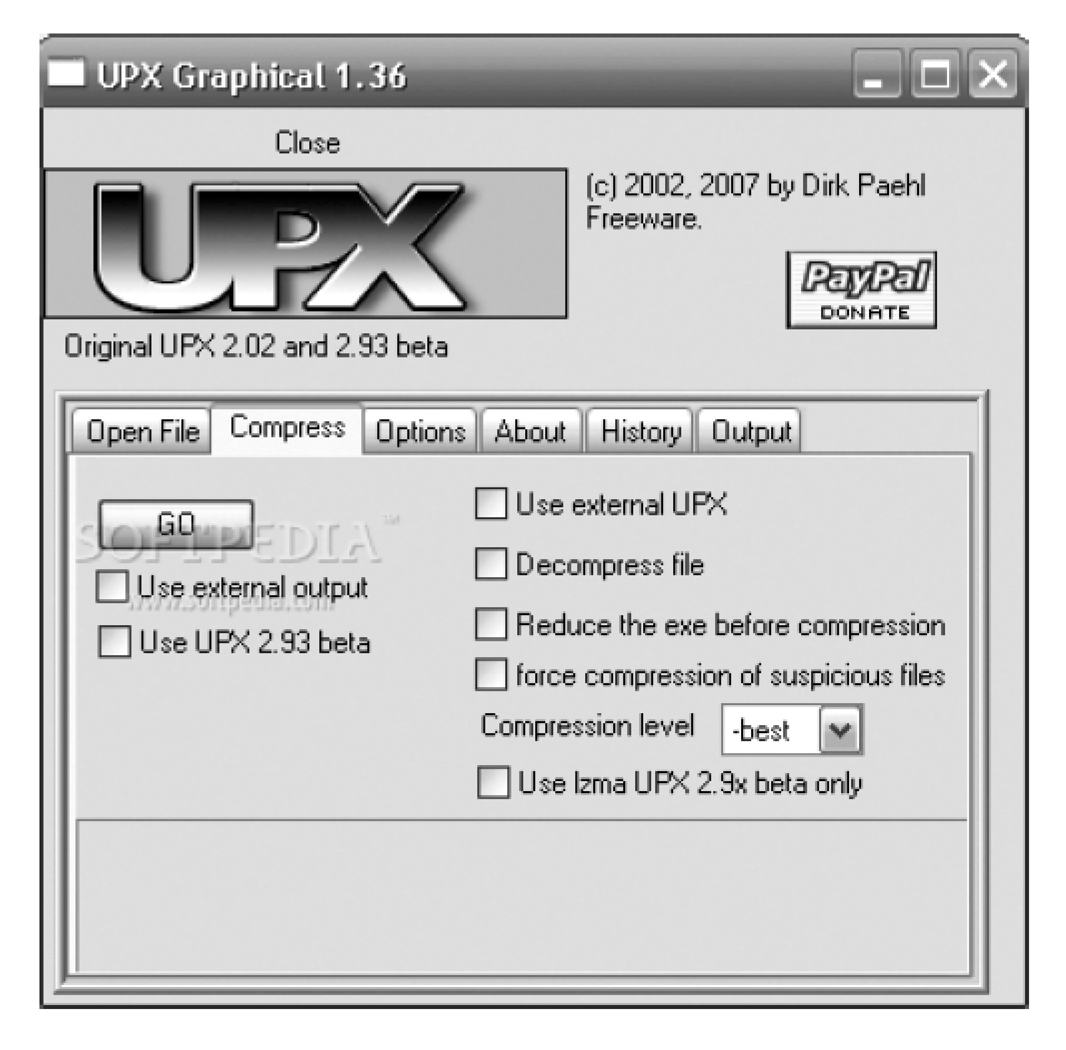


图 4-3　UPX 运行界面

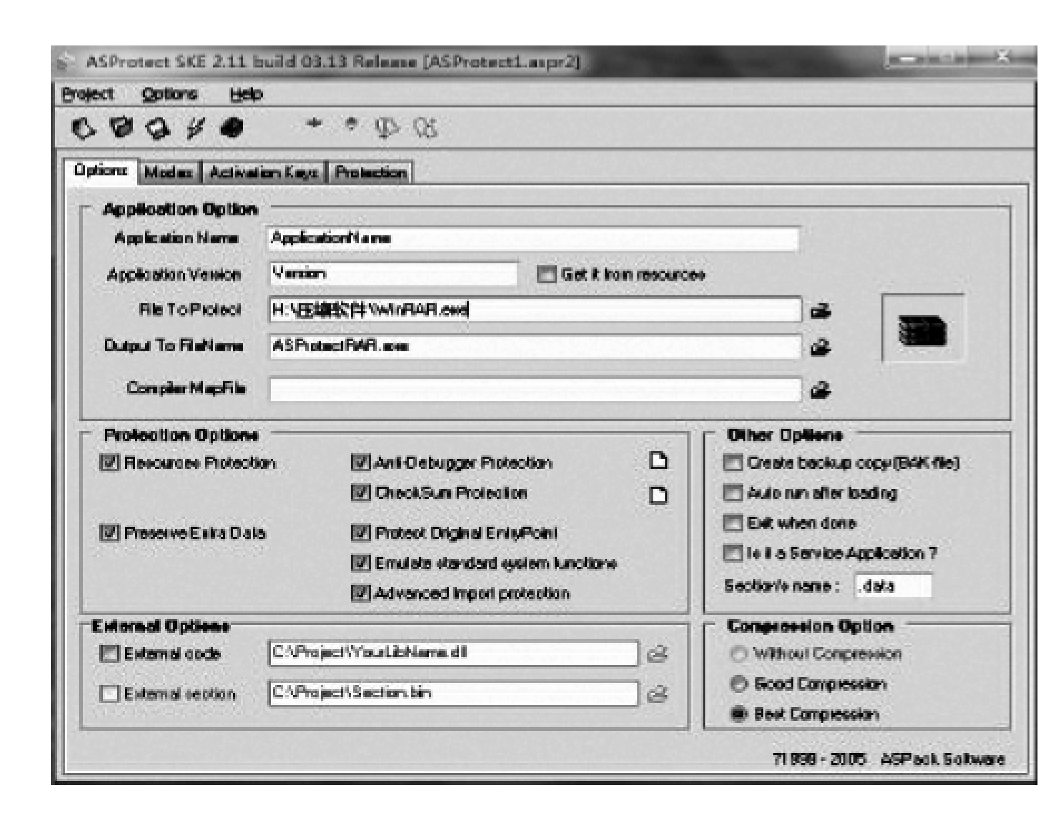


图 4-4　ASProtect 运行界面

4. tElock

tElock 是一款免费的外壳保护工具。压缩引擎使用 UPX 内核，可压缩保护 32 位可执行文件 EXE、DLL 和 OCX。它使用了各种 Anti-Debug 技术、SMC 技术、重整覆盖、重整 Reloc、自建输入表和产生任意区块名等保护技术，其运行界面如图 4-5 所示。

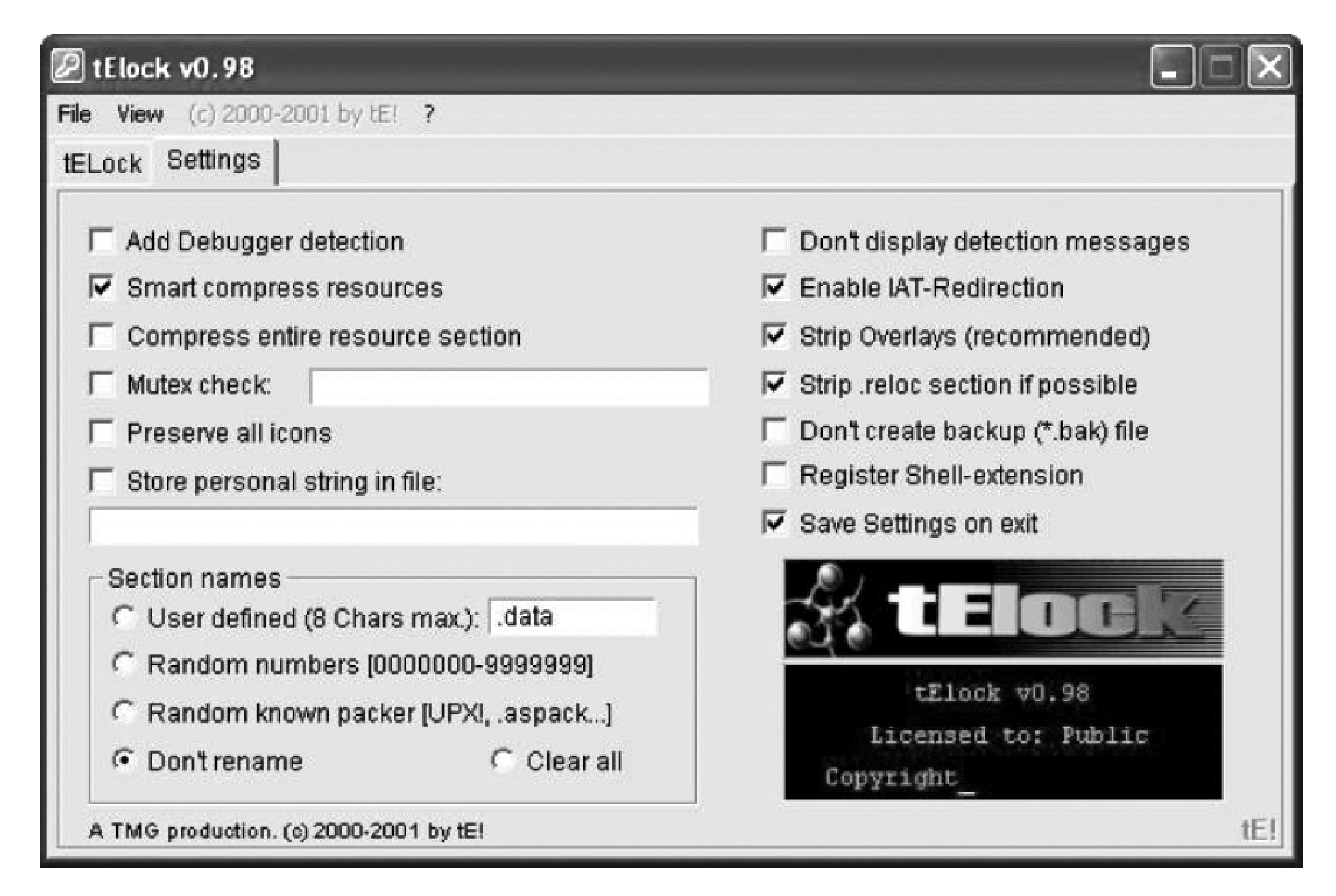


图 4-5　tElock 运行界面

4.4.3　软件脱壳工具

有加壳就必有脱壳，软件脱壳就是对软件加壳的逆操作，把软件中存在的壳去掉，删

除其中的干扰信息和保护限制，还原软件的本来真实面目。如果脱壳后的软件能正常运行，并且没有功能损耗和其他的限制，则说明脱壳成功。

按照脱壳方式的不同，可以分为工具脱壳和手动脱壳，工具脱壳是指在脱壳过程中，采用专业的脱壳软件，对已加壳的 EXE、DLL 文件破解；手动脱壳是指在脱壳过程中，主要依靠破解者的专业知识，辅助以相应的软件，对已加壳的 EXE、DLL 文件破解，对破解者的专业知识要求很高。一般的压缩壳，如 ASPack、UPX 等都有专用的脱壳机；而保护壳，如 ASProtect、Armadillo 一般很少有脱壳机，必须手工脱壳。

脱壳软件主要分为专用脱壳软件和通用脱壳软件。专用脱壳软件只能脱掉特定的一种或两种加壳软件所加的壳，因为它是专门针对某种加壳软件的某个版本而制作的。通用脱壳软件具有通用性，可以脱掉多种不同的壳。

专用脱壳软件按照其针对加壳软件的流行程度大致分为 4 种：脱 ASPack 壳软件、脱 UPX 壳软件、脱 PECompact 软件和其他专用脱壳软件。

1. 脱 ASPack 壳软件

针对 ASPack 壳的脱壳软件主要有 UnASPack、CASPR 和 ASPackDie。

（1）UnASPack 软件采用图形界面，操作简单，运行软件后选取待脱壳的软件即可，脱壳后的文件特别干净，但目前只能脱 ASPack2.1 及其以前的版本，其运行界面如图 4-6 所示。

（2）CASPR 脱壳软件的优点是可以脱 ASPack2.1.2 版本以前 ASPack 任何版本的壳，脱壳能力极强，其缺点是 DOS 界面。

（3）ASPackDie 软件的优点是支持从 ASPack2000 到 ASPack2.1.2b 版的壳，缺点是不支持旧版壳。使用方法为运行软件后选取待脱壳的软件即可完成脱壳工作。

2. 脱 UPX 壳软件

脱 UPX 壳最好使用与加壳软件所用版本相同的 UPX 脱壳软件 UPXShell，它是最好的脱 UPX 壳的程序，并且此软件和 UPX 一样，都是免费软件，UPXShell 支持最新版的 UPX 主文件，其运行界面如图 4-7 所示。

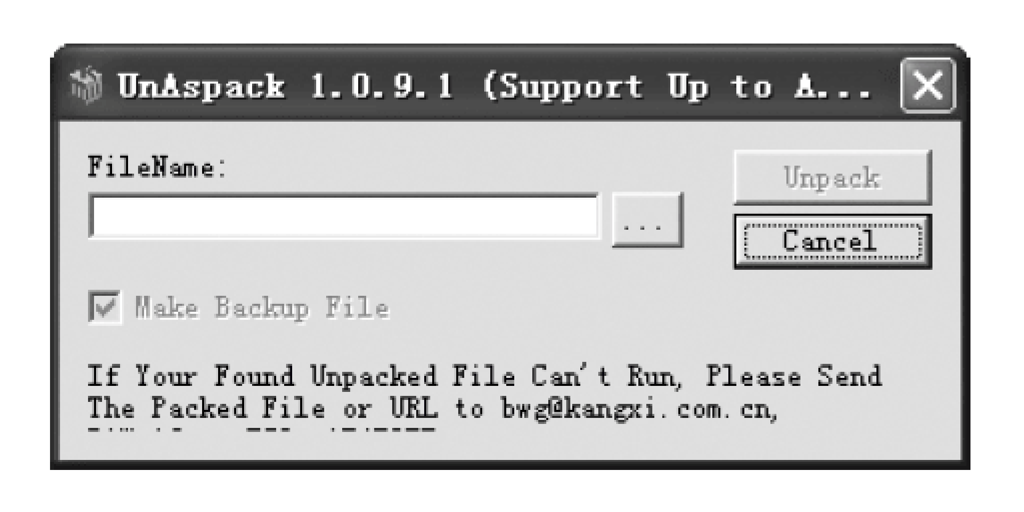


图 4-6　UnASPack 运行界面

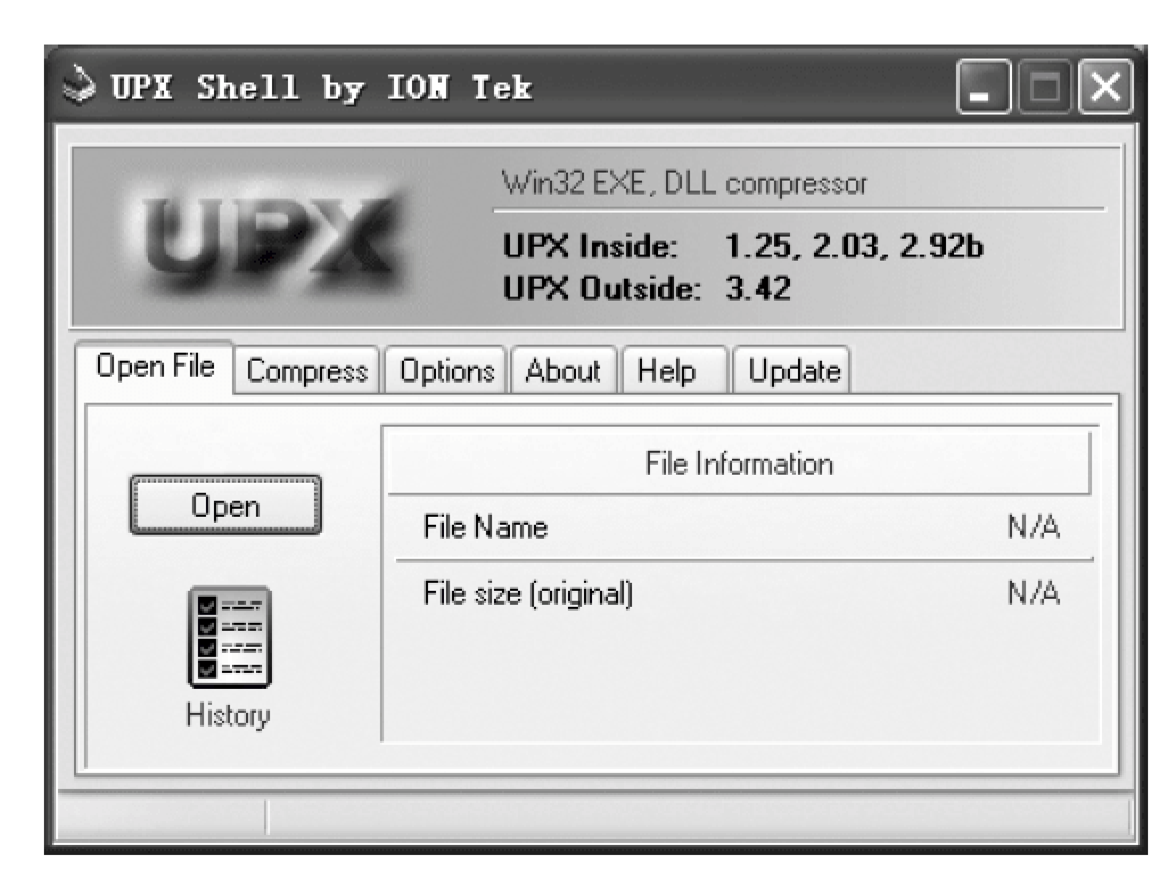


图 4-7　UPXShell 运行界面

3. 脱 PECompact 软件

UnPECompact 是专门用来脱 PECompact 加密的脱壳工具。

4. 通用脱壳软件

较常见的通用脱壳软件有 ProcDump、UN-PACK 等。

ProcDump 是一款功能强大的脱壳工具，它有一个 script.ini 的脚本文件，可以编写新的脚本存入 script.ini 文件来对付新的加壳软件，这个特点是别的脱壳软件所不具备的，ProcDump1.6.2 为最终版本，尽管作者早已停止升级，但它却具有持久的生命力，是进行脱壳的必备解密工具。

UN-PACK 是 Pile Analyzer and Unpacker 的简称，是著名的脱壳软件破解组织 Ug2001 推出的一款脱壳工具集合，通过统一的界面，可以自动侦测目标软件究竟是被何种加壳软件加的壳，并提示相关的文件信息，最后提示用户可以用何种工具脱壳。该软件集类型分析与自动脱壳功能于一身。

4.5 软件防盗版技术

通过某种技术，使得操作系统的复制方法，甚至磁盘复制软件不能将软件完整复制，或者复制后不能安装运行使用，这种技术被称为软件的防盗版技术。

本节简要介绍软件防盗版技术的定义与分类，并重点介绍磁盘防复制技术与光盘防复制技术。

4.5.1 软件防盗版的思想

盗版软件主要是通过非法复制和非法安装运行来实现的。非法复制是盗版软件能得以传播的根源，而非法安装运行才是盗版软件最终的目的。如果从技术上能防止非法复制，就切断了盗版软件的盗版之源。然而，非法用户可以“借”合法用户的软件产品安装使用，显然仅防止非法复制达不到软件保护的目的。因此，防止软件非法安装运行才是防止软件盗版的最终解决方案。

针对防盗版技术的具体实现细节，可以使用纯硬件方式、纯软件方式或软硬件结合的方式。纯硬件方式成本相对比较高，但灵活性差，破译相对难一些；纯软件方式几乎不需要增加任何成本，灵活性好，但破译比较容易；软硬件结合方式是前两种方式的结合，具有较好的灵活性，破译难度随软件的复杂程度而变。

防止软件非法复制必须从软件发行载体入手。目前软件发行的载体主要有软磁盘、光盘以及计算机网络。软磁盘由于其容量较小，仅用于小型软件或软件密钥盘；光盘以其大容量、低成本以及耐用等特点，是目前最理想的软件发行载体；而计算机网络由于其灵活性较好，也逐渐成为小型共享软件发行的首选载体之一。

防止软件非法安装运行技术通常采用的是本章已介绍过的加密技术的原理，即使用密钥将软件加密。用户可以随便复制，但是在安装运行之前需要使用密钥解密，才能正确

运行软件。

下面将从软件发行载体这一角度入手，重点介绍磁盘防复制技术和光盘防复制技术，如何通过网络来保护软件应用的安全将在其他章节中介绍。

4.5.2 磁盘防复制技术

磁盘防复制技术是前几年使用最广泛的技术，KV杀毒系列、瑞星密钥盘等都使用这种技术防复制。磁盘防复制技术比较通用的是对软磁盘进行各种非标准处理，使用通用的软磁盘读写方法无法对它实现正常读写。常见的方法有：①在软磁盘上制作一个永久性的无法复制的硬标志，然后在被保护软件中加入一段对此硬标志的识别程序。如激光打孔加密法、电磁加密法、掩膜加密法等防复制技术就是采用这种方法；②对软磁盘的某些磁道或扇区进行特殊格式化，把密钥放在经过特殊格式化的磁道和扇区中，如额外扇区法、超级扇区法、未格式化扇区法、额外磁道法、异常ID法、磁道接缝指纹法等防复制技术均是采用这种方法。

下面介绍几种常用的磁盘防复制技术。

1. 使用异常的ID参数

当磁盘被格式化后，每个扇区都有一个识别标志(ID)字段，它记录着该扇区(360K软磁盘，下同)的磁道号C(0～39)、磁头号H(0～1)、扇区号R(1～9)和长度N(2)。ID字段是磁盘在格式化时被写入的，在写入时不作正确性检查，所以可以在格式化磁盘时任意修改ID字段中的内容。当要读写磁盘时，就要求将被读取扇区的ID字段与相应的读写参数(是标准DOS格式时，由系统默认的INT1E提供该标准格式参数)进行比较，只有当两者相同时，读写操作才能成功。如果使用了异常的ID参数格式化出了一个磁道或扇区，那么在读写该磁道或扇区时，必须给出格式化时所用的ID参数才能读写成功，这个磁道或扇区就被称作为指纹，这种异常的ID参数加密法能成功地防止各类DOS标准格式复制程序，所以在1983—1985年中得到了广泛采用，但是它最终没有逃脱COPYⅡPC和COPYWRIT的威慑，于1986年开始单纯使用异常ID参数的反复制技术已经销声匿迹了。

2. 弱位技术

磁盘是一种通过不同的磁化单元来记录信息的磁记录设备，它记录的信息有两种可能性，即“1”或“0”，但如果在写盘时采用了特殊技术，使得所记录的信息比1信号弱些，比0信号强些，这样就形成了反复制技术中的弱位技术，这种技术具有较强的反复制能力，这是因为当磁盘机从原盘上读取数据时，读出的数据非1即0，对弱位也不例外，可是弱位中存放的是一种非1非0的数据，所以它存在多次读取的结果不一致的特点，如果复制程序只按某一次读取的数据进行复制的话，必然使复制盘中不含弱位。弱位技术是一种构思比较巧妙的反复制技术，但是关于它的制作方法却很少公开，不过可以利用工具软件EXPLORER来制作，有兴趣的读者可以研究一下。

3. 宽磁道技术

磁盘机的磁头由读写磁头和消磁磁头组合而成,其中的读写磁头用来读写磁道,而在读写磁头外侧的消磁磁头主要用于抹除读写磁头所产生的多余磁场,以减少磁道间的数据干扰。宽磁道技术则是针对磁盘机磁头的这种组合来设计的,它的具体实现是利用一种能同时在两个或更多的磁道上写数据的宽磁头,在两个相邻的磁道上写上相同的数据,甚至可在这两个磁道之间的间隙中写上相同的数据(这是相对比较窄而且具有消磁磁头的普通磁头无论如何也做不到的),以此建立一个较普通磁道至少宽一倍的宽磁道,在用普通磁头读取该磁道时可以使磁头在这个宽磁道上(实际是两个磁道)来回步进,这样就可以读取磁道及磁道间隙上的所有数据,但如果用普通磁头复制这类宽磁道时,由于消磁磁头的存在始终会造成一个间隙,所以根本无法构造宽磁道。

4. CRC 错误法

循环冗余校验码 CRC 是软磁盘控制器 FDC 在向磁盘写入数据时自动生成的。它位于 ID 字段和数据字段之后,占有两个字节,在正常时,软磁盘控制器所产生的 CRC 校验码都是正确的,只有在软磁盘有物理性损伤或缺陷时才会产生错误的 CRC 校验码。针对这个特点人们又发明了一种新颖的反复制技术——人为生成错误的 CRC 校验码,就是在写入数据时,人为地在某一个扇区或几个扇区产生 ID 字段或数据字段的错误校验码。在复制有 CRC 错误的扇区时,由于软磁盘控制器 FDC 在正常的情况下,本身绝对不会产生错误的 CRC 校验码(除非软磁盘有缺陷),所以肯定也不可能复制人为生成的错误的 CRC 校验码。在加密系统运行时,可以对软磁盘的特定扇区进行检查,如果发现该扇区中有错误的 CRC 检验码,则正常运行,反之则退出。生成错误的 CRC 校验码的方法是当正在向某一磁道的某一个扇区写入数据的时候(注意没有结束),人为地复位软磁盘控制器,打断磁盘的数据写入过程,以导致软磁盘正常的数据写入混乱,从而人为地生成了错误的 CRC 校验码(正常的 CRC 校验码是在软磁盘控制器写完某扇区的最后一个字节的同时生成并写入软磁盘的)。这类方法是一种运用较广泛的防复制技术,早期的中、英文 dBASEⅢ及 Lotus1-2-3 等几种常见的应用软件皆采用了这类防复制技术,如果稍加修改可以防止 COPYWRIT 等高级复制工具的复制。

5. 针孔防复制技术

软盘加密在经过一段时间的发展后,人们提出了针孔防复制技术。

早在 20 世纪 80 年代末期,就有人开始尝试用针孔来代替造价昂贵的激光孔了,至 20 世纪 90 年代初期,甚至有人提出用针孔来复制激光加密孔,以达到复制软磁盘控制器根本无法生成的激光孔的目的。从它发展的过程来看,针孔反复制技术的确有着其吸引人的一面,如生成的损伤区域小,造价十分低廉等,所以针孔反复制技术有着“仿激光加密技术”的美称,但是它还是有些致命弱点的,如损坏磁头、制作效率不高等,所以说它要取代激光加密技术是不切合实际的。

6. 掩膜反复制技术

激光与针孔防复制技术都是损坏了磁盘的磁性介质,破坏了磁盘的光洁度,对软磁盘驱动器的磁头都有一定程度的磨损,为了弥补这个不足,掩膜反复制技术便应运而生了。掩膜反复制技术是在磁介质的某一块区域上镀上一层膜,从而使该区域不能正常记录信息,也使复制工具无法识别,导致复制失败。掩膜反复制技术与激光加密技术一样,有极高的可靠性,而且是一种很有前途的指纹制作技术。

4.5.3 光盘防复制技术

光盘是商业软件最常用的传播载体之一,绝大多数商业软件最终都以光盘的形式发放到用户手中。目前计算机软件市场上光盘盗版的现象非常严重,光盘保护是软件版权保护非常重要的一个方面。光盘保护主要是防止光盘复制和硬盘复制。

1. 防止光盘复制

防止光盘复制是指防止对光盘中数据进行复制,阻碍盗版光盘的生产。

一般可以通过修改光盘的ISO结构,使文件目录隐藏,或者文件大小异常,或者将目录以文件方式显示,阻碍光盘复制的行为。

需要更为可靠的保护可以在修改光盘ISO结构的同时为光盘添加开锁程序和不可复制的开锁信息。开锁程序中包含一串密文,开锁程序对开锁信息进行加密运算后与内部密文进行比较,两者相符才跳转至正确的入口启动软件。要实现开锁信息的不可复制性,可以采用的手段有利用指纹或数字签名作为开锁信息,将一串代码刻录至光盘上的特殊位置,这些位置上的数据无法直接读出,只有开锁程序能检测到此指纹的存在并验证其有效后才能读出,如采用激光加密技术将特殊刻录的激光孔硬标志作为“指纹信息”;利用光盘的固有物理属性作为开锁信息。

2. 防止硬盘复制

防止硬盘复制是指防止将光盘程序复制到硬盘中运行。可以在软件运行过程中,判断光驱中是否存在特定文件,或者在运行中加载光盘中的部分代码或数据,这样用户即使将光盘数据复制到硬盘,没有相应的光盘,软件也不能正常运行。

4.6 常用的软件保护方法

前面分类介绍了软件的安全防护技术,本节将集中介绍几种常用的软件保护方法。

4.6.1 序列号保护方法

1. 序列号保护机制

当用户从网络上下载某个shareware——共享软件后,一般都有使用时间上的限制,当过了共享软件的试用期后,用户必须到这个软件的公司去注册后方能继续使用。注册

过程一般是用户把自己的私人信息(一般主要指姓名)连同信用卡号码告诉给软件公司,软件公司会根据用户的信息计算出一个序列码,在用户得到这个序列码后,按照注册需要的步骤在软件中输入注册信息和注册码,其注册信息的合法性由软件验证通过后,软件就会取消本身的各种限制,这种加密实现起来比较简单,不需要额外的成本,用户购买也非常方便,在互联网上的软件80%都是以这种方式来保护的。

软件验证序列号的合法性过程,其实就是验证用户名和序列号之间的换算关系是否正确的过程。最基本的验证方式有下面两种:

(1) 由姓名生成注册码。

按用户输入的姓名来生成注册码,再同用户输入的注册码比较,公式如下:

序列号=F(用户名)

这种方法等于在用户软件中再现了软件公司生成注册码的过程,存在不安全性,因为不论换算过程多么复杂,解密者只需把换算过程从程序中提取出来就可以编制一个通用的注册程序。

(2) 由注册码生成姓名。

通过输入注册码来验证用户名的正确性,公式表示如下:

用户名=F逆(序列号)(如ACDSEE)

这是软件公司注册码计算过程的反算法,如果正向算法与反向算法不是对称算法的话,对于解密者来说,的确有些困难,但这种算法相当不好设计。于是有人考虑到以下的算法:

F1(用户名)=F2(序列号)

F1、F2是两种完全不同的算法,但用户名通过F1算法的计算出的特征字等于序列号通过F2算法计算出的特征字,这种算法在设计上比较简单,保密性相对以上两种算法也要好得多。如果能够把F1、F2算法设计成不可逆算法的话,保密性相当好;可一旦解密者找到其中之一的反算法的话,这种算法就不安全了。

一元算法的设计看来再如何努力也很难有太大的突破,有人考虑使用二元算法。

特定值=F(用户名,序列号)

二元算法看上去相当不错,用户名与序列号之间的关系不再那么清晰了,但同时也失去了用户名与序列号的一一对应关系,软件开发者必须自己维护用户名与序列号之间的唯一性,但这不是难以办到的事,建个数据库就可以解决。当然也可以根据这一思路把用户名和序列号分为几个部分来构造多元的算法。

特定值=F(用户名1,用户名2,…,序列号1,序列号2,…)

现有的序列号加密算法大多是软件开发者自行设计的,大部分相当简单,而且有些算法作者虽然下了很大的工夫,效果却往往得不到它所希望的结果。

2. 如何攻击序列号保护

要找到序列号,或者修改掉判断序列号之后的跳转指令,最重要的是要利用各种工具定位判断序列号的代码段。这些常用的API包括GetDlgItemInt,GetDlgItemTextA,GetTabbedTextExtentA,GetWindowTextA,Hmemcpy(仅限于Windows 9×),lstrcmp,

lstrlen，memcpy（仅限于NT/2000）。

（1）数据约束性的秘诀。

这个概念是+ORC提出的，只限于用明文比较注册码的保护方式。在大多数序列号保护的程序中，那个真正的、正确的注册码或密码（password）会于某个时刻出现在内存中，当然它出现的位置是不定的，但多数情况下它会在一个范围之内，即存放用户输入序列号的内存地址±0X90字节的地方。这是由于加密者所用工具内部的一个Windows数据传输的约束条件决定的。

（2）Hmemcpy函数（俗称万能断点）。

函数Hmemcpy是Windows 9×系统的内部函数，位于KERNEL32.DLL中，它的作用是将内存中的一块数据复制到另一个地方。由于Windows 9×系统频繁使用该函数处理各种字串，因此用它作为断点很实用，它是Windows 9×平台最常用的断点。在Windows NT/2000中没有这个断点，因为其内核和Windows 9×完全不同。

（3）S命令。

由于S命令忽略不在内存中的页面，因此可以使用32位平面地址数据段描述符30h在整个4GB（0～FFFFFFFFh）空间查找，一般用在Windows 9×。

具体步骤为：先输入姓名或假的序列号（如78787878），按Ctrl+D切换到SoftICE下，再下搜索命令：

```
s 30:0 L ffffffff '78787878'
```

会搜索出地址：ss：ssssssss（这些地址可能不止一个），然后用bpm断点监视搜索到的假注册码，跟踪一下程序如何处理输入的序列号，就有可能找到正确的序列号。

（4）利用消息断点。

在处理字串方面可以利用消息断点WM_GETTEXT和WM_COMMAND。前者用来读取某个控件中的文本，例如拷贝编辑窗口中的序列号到程序提供的一个缓冲区里；后者则是用来通知某个控件的父窗口的，例如当输入序列号之后单击OK按钮，则该按钮的父窗口将收到一个WM_COMMAND消息，以表明该按钮被点击。

```
BMSG xxxx WM_GETTEXT （拦截序列号）
BMSG xxxx WM_COMMAND （拦截 OK按钮）
```

可以用SoftICE提供的HWND命令获得窗口句柄的信息，也可以利用Visual Studio中的Spy++实用工具得到相应窗口的句柄值，然后用BMSG设断点拦截。例如：

```
BMSG 0129 WM_COMMAND
```

4.6.2 注册文件保护（KeyFile保护）

1. KeyFile保护的思路

KeyFile（注册文件）是一种利用文件来保护软件的方式。KeyFile一般是一个小文件，可以是纯文本文件，也可以是包含不可显示字符的二进制文件，其内容是一些加密过

或未加密的数据，其中可能有用户名、注册码等信息。文件格式由软件作者自己定义。试用版软件没有注册文件，当用户向作者付费注册之后，会收到作者寄来的注册文件，其中可能包含用户的个人信息。用户只要将该文件放入指定的目录，就可以让软件成为正式版。该文件一般是放在软件的安装目录中或系统目录下。软件每次启动时，从该文件中读取数据，然后利用某种算法进行处理，根据处理的结果判断是否为正确的注册文件，如果正确则以注册版模式来运行。

为增加破解难度，可以在 KeyFile 中加入一些垃圾信息；对于注册文件的合法性检查可分散在软件的不同模块中进行判断；对注册文件内的数据处理也尽可能采用复杂的算法。

2．Key File 破解的思路

为了更好地利用 KeyFile 保护，不仅要了解 KeyFile 保护方式的原理，还要了解破解 KeyFile 保护的方法。KeyFile 保护方式可以通过创建假的 KeyFile 文件来进行破解。一般来讲，KeyFile 文件都是“*.key”格式，因此可以在假的 KeyFile 中输入一些特别的语句，作为识别的标志。然后通过动态调试工具在一些特殊的 API 函数上设置断点，进行断点拦截，找出 KeyFile 正误的判断函数，这样就容易进行破解了。

具体步骤如下：

（1）借助 Filemon 等监视工具对文件的操作，找到 KeyFile 的文件名。当软件读取 KeyFile 时，Filemon 会显示对应的 KeyFile 文件名。这样就可以知道 KeyFile 的文件名了。

（2）创建一个假的 KeyFile 文件。编辑和修改 KeyFile 文件的最好工具是十六进制，如 W32DASM、HexWorkshop，普通的文本编辑工具不太适合。

（3）在 Windows 下，用一些特殊的 API 函数设置断点，这些 API 函数包括 ReadFile、CreateFileA、_lopen 和 FindFirstFileA 等文件操作函数，跟踪分析程序是如何操作注册文件的，构造一个正确的注册文件，或者写出自动生成注册文件的程序，或者修改程序指令跳过对注册文件的检查，从而得到一个注册版本的软件。

3．Windows 下破解 Key File 几个常用的函数

（1）函数 ReadFile。

作用：从文件中读出数据。

参数：其中 Long，非零表示成功，零表示失败。

函数用法示例：

```
BOOL ReadFile(
HANDLE hFile,                           //Long,文件的句柄
LPVOID lpBuffer,                        //Any,用于保存读入数据的一个缓冲区
DWORD nNumberOfBytesToRead,             //Long,要读入的字符数
LPDWORD lpNumberOfBytesRead,            //Long,从文件中实际读入的字符数
LPOVERLAPPED lpOverlapped               //数据结构地址
```

```
);
```

（2）函数 CreateFileA。

作用：可打开和创建文件、管道、邮槽、通信服务、设备以及控制台。

函数用法示例：

```
HANDLE CreateFileA(
LPCTSTR lpFileName,                          //String,要打开的文件的名字
DWORD dwDesiredAccess,                       //允许对设备进行读写访问
DWORD dwShareMode,                           //共享模式
LPSECURITY_ATTRIBUTES lpSecurityAttributes
        //指向一个 SECURITY_ATTRIBUTES 结构的指针,定义了文件的安全特性(如果操作系统支持)
DWORD dwCreationDistribution,                //如何创建文件
DWORD dwFlagsAndAttributes,                  //文件特性
HANDLE hTemplateFile
            //Long,如果不为零,则指定一个文件句柄。新文件将从这个文件中复制扩展属性
);
```

（3）函数_lopen。

作用：以二进制模式打开指定的文件。

函数用法示例：

```
HFILE lopen(
LPCSTR lpPathName,                           //欲打开文件的名字
int iReadWrite                               //访问模式和共享模式常数的一个组合
);
```

（4）函数 FindFirstFileA。

作用：根据文件名查找文件。

函数用法示例：

```
HANDLE FindFirstFile(
LPCTSTR lpFileName,          //欲搜索的文件名。可包含通配符,并可包含一个路径或相对路径名
LPWIN32_FIND_DATA lpFindFileData //WIN32_FIND_DATA,这个结构用于装载与找到的文件有关的信息。
该结构可用于后续的搜索
);
```

4.6.3 软件限制技术

目前,许多应用程序都有在一定限制条件内免费使用的功能,利用该功能可以有效限制非法用户的使用,同时,还可以使合法用户在充分了解软件优缺点的基础上,再决定是否购买。实现这种功能的方法为软件限制技术。软件限制技术的利用在保护正版软件的基础上,既有效地扩大了软件的使用范围,又给用户提供了进行充分选择的机会。

软件限制技术有很多种,如利用注册表限制程序使用的天数,例如限制使用 30 天;利用注册表限制程序使用的次数,例如限制使用 45 次;设定程序使用的截止日期,例如设截

止日期为 2013 年 6 月 30 日；限制每次使用程序的时间，例如一次允许使用 50 分钟。限制使用程序的部分功能，例如菜单中选项是灰色的功能无法使用。这些软件限制技术既可以单独使用，也可以几个同时使用实现综合保护。下面介绍两种具体的限制技术。

1. 时间限制技术

一般使用这类保护的软件都有时间上的限制，如使用期 30 天，当过了共享软件的使用期后，就不予运行，只有向软件作者付费注册后才能得到一个无时间限制的注册版本。这种保护方式的程序很多，安装时，在系统中做上标记，例如将系统的安装时间存放在一个文件中，每次运行时用系统的当前时间和安装时间作比较，判断用户能否使用。

为了更好地理解软件限制技术的保护原理，需要了解破除软件限制技术的方法。针对不同的时间限制技术，有不同的去除时间限制的方法。例如最典型的 30 天限制的一种情况，解除限制的方法为，用 W32DASM 将其源程序反汇编后的代码为：

```
mov ecx,1E;                  //把 1E(30天十进制)放入 ecx
mov eax,[esp+10];            //把用过的天数放到 eax
cmp eax,ecx;                 //在此比较用过的天数和 30的大小关系
jl…                          //跳转到相应的代码继续执行
```

此时只需把“mov eax,[esp+10]”改成“mov eax,1”即可。

2. 功能限制技术

这种程序一般是 DEMO 版或菜单中部分选项是灰色。有些 DEMO 版本的部分功能根本就没有，而有些程序功能全有，只要注册后才正常。使用这些 DEMO 程序部分被禁止的功能时，会跳出提示框，说这是 DEMO 版等，它们一般都是调用 MessageBox[A]或DialogBox[A]等函数。

保护与破解过程常用的 API 函数有 EnableMenuItem 和 EnableWindow 等。因此可以用 W32DASM 反汇编目标程序，然后在代码中查找字符串：“Function Not Avaible in Demo” 或“Command Not Avaible”或“Can’t save in Shareware/Demo”等，截获这次 CALL 调用，即可破解目标软件 DEMO 版的限制功能。

另外，如果菜单中部分选项是灰色的不能用，一般通过 EnableMenuItem 和 EnableWindow 两种函数实现。

(1) EnableMenuItem。

该函数主要用来允许、禁止或变灰指定的菜单条目，例如通过下面的程序来实现：

```
BOOL EnableMenuItem (
HMENU hMenu,                 //菜单句柄
UINT uIDEnableItem,          //菜单 ID,形式为：允许,禁止,或变灰
UINT uEnable                 //菜单项目
);
Returns
```

在 ASM 代码形式如下：

```
PUSH uEnable                    //uEnable=0则菜单选项允许
PUSH uIDEnableItem
PUSH hWnd
CALL [KERNEL32! EnableMenuItem]
```

(2) EnableWindow。

该函数主要用来允许或禁止鼠标和键盘控制指定窗口和条目(禁止时菜单变灰),例如:

```
BOOL EnableWindow(
HWND hWnd,                      //窗口句柄
BOOL bEnable                    //允许/禁止输入
);
Returns
```

如果窗口以前被禁止则返回 TRUE,否则返回 FALSE。

4.6.4 加密狗

1. 加密狗的构成

加密狗是插在计算机并行口上的软硬件结合的软件加密产品。加密狗一般都有几十或几百字节的非易失性存储空间可供读写,有的内部还增添了一个单片机。软件运行时通过向并行口写入一定的数据,判断从并行口返回密码数据正确与否来检查加密狗是否存在。加密狗包括加密代码程序和“密钥”(亦称加密盒)两部分。加密代码程序检查“密钥”是否存在,是否正确,在无误的情况下,去执行正常功能的应用程序。“密钥”中存放了“密码”,用硬件电路实现加密。

2. 加密狗的工作原理

为了防止程序被非法复制,加密狗所做的加密保护措施一般都包括两部分。首先是要有保存密码数据的载体,即密钥;其次是夹杂在应用程序中的主机检查程序,即加密代码。密钥应该能保证不易被解密、复制;如一般用磁盘做加密时,加密部分无法用一般的工具复制。另外,当检查程序用特殊方法去读密码时,密码应该能很容易地被读出,而不致影响应用程序的正常执行。当发现密码不对或密钥不存在时,就让主机挂起、重新启动或采用其他的措施。

3. 市场上常见的加密狗产品

平时常见的狗主要有“洋狗”(国外狗)和“土狗”(国产狗)。这里“洋狗”主要指美国的彩虹和以色列的 HASP,“土狗”主要有金天地(现在与美国彩虹合资,叫彩虹天地)、深思、坚石。总地来说,“洋狗”在软件接口、加壳、防跟踪等“软”方面做得没有“土狗”好,但在硬件上绝对无法匹及;而“土狗”在“软”的方面做得绝对称得上世界第一,许多技术,如噪音、自检测、算法可变、码表变换等,可以说都很先进,而在硬件上不及国外,只要稍有单片机

功力的人，都可复制。

加密狗技术发展很快，针对不同的应用场合有不同的类型，可以分为强劲狗、微狗、USB狗、软件狗、网络狗、卡式狗等。

4.6.5　反动态跟踪技术

软件的反动态跟踪就是防止解密者利用程序调试工具跟踪软件的运行、窃取软件源码、取消防复制和加密功能实现对软件的动态破译。

随着计算机加密技术的发展，它的对立面——解密技术也应运而生并发展着。因此除了对程序进行可靠的加密外，还要有较好的反跟踪措施来防止非法复制者对所研制的软件进行解密。

1. 有效的反动态跟踪加密软件的特性

一个有效的反动态跟踪措施的加密软件应该具备以下三个特性：

(1) 识别程序是不可跳跃的，不执行识别程序，程序就无法执行。

(2) 识别程序是不可动态跟踪执行的，并且是复杂和隐蔽的，如果强行跟踪，程序就无法执行。

(3) 不通过识别程序的译码算法，密码是不可破译的。

实现特性(1)可以通过某种信息加密算法，将被保护程序本身进行加密处理，全部转换成密码，只有当识别程序将保护程序的代码从密码形式转换为明码形式后，被保护程序才能正常运行。于是解密者就无法越过识别程序来观察和运行被保护程序。

实现特性(2)可以采用一种识别程序的译码算法，它的运行必然造成解密者动态跟踪环境的破坏。这样，解密者若不执行识别程序的译码算法，就无法观察和运行被保护的程序。

此外，识别程序还可以对运行的状态做进一步的判断，若判定加密程序是在调试程序控制下运行，则立即停止对程序的运行，或将跟踪引入歧途。

2. 反动态跟踪技术的实现途径

反动态跟踪技术总地来说有两种途径来破坏跟踪。

(1) 通过暂时破坏软件调试和动态跟踪软件的某些功能和运行环境，使跟踪者跟踪几步就死机、机器自启动或者屏幕混乱；

(2) 利用反穷举法、程序流动态控制措施、逆指令流技术等，在程序中安排大量的陷阱，使跟踪者在筋疲力尽前不能进行实质有效的跟踪。例如在程序中故意地安排大量的循环、多出口程序，它们不完成任何有用功能，只是进行多次循环。

4.6.6　软件水印

软件水印是嵌入到程序当中的秘密消息，这些消息应能方便可靠地提取出来，以证明软件的所有权，并且具有在保证程序功能的情况下不能或难以去除该消息的功能。该技术可提供所有者鉴别、所有权验证、操作跟踪、复制控制等服务，是密码学、软件工程、算法设计、图论等学科的交叉研究领域。简单地说，软件水印是用水印的思想实施软件保护。

从软件水印的用途来看，其具有以下一些应用：

(1) 软件版权申明(authorship):通过软件水印申明软件的版权,软件中的水印信息可以被任何合法的用户(公开水印密钥)提取。软件用户可以通过该水印判断所使用的软件是否为正版软件。

(2) 软件版权证明(authentication):通过软件水印证明软件的版权,软件中的水印信息仅能被软件开发者(拥有水印密钥)提取,该水印信息可以证明软件的所有权。当两个公司都称某软件是自己公司的软件时,软件版权证明水印可以证明软件的所有权,从而揭穿盗版者的谎言。

(3) 盗版源的跟踪:在分发给不同使用者的软件中嵌入的水印信息各不相同(不同的信息是软件的指纹),当盗版行为发生时,可以根据软件的指纹寻找盗版软件是从哪个使用者流传出去的,从而定位盗版源。

(4) 非法复用软件模块的发现:如果整个软件被盗用,常常是容易发现的;但当仅有某个模块给非法复用时,常常是难以发现的,软件水印可以用于发现与检测这种情况下的盗版行为。

(5) 盗版自报告:Easter Egg 软件水印利用了软件可运行的特点,把水印检测器嵌入到软件中,当检测器运行时,可以通过检查软件的生存环境(例如主机 IP 等),判断该软件的生存环境是否构成盗版行为,进而在可能的情况下,通过网络主动报告盗版行为。

(6) 盗版自发现:随着计算机网络的迅速发展,通过网络分发软件成为软件分发的一种重要手段,这就给软件盗版的自发现提供了可能。可以利用网络爬虫技术搜索 Internet 网上的软件,并检测这些软件当中的水印信息,从而自动地发现盗版行为。

4.7 应用实例

在学习软件安全防护技术相关理论之后,本节将介绍两个常用的软件安全技术的应用实例,以便读者更快速地掌握几种软件加密工具的使用方法。

4.7.1 软件加壳脱壳

软件加壳是保护代码或维护软件产权等利益所常用到的手段。目前有很多加壳与脱壳工具,脱壳又有自动脱壳和手动脱壳之分,下面以 ASPack 2.12 和 ASPackDie 为 AccessDriver 的执行程序加壳和脱壳为例,介绍软件加壳和脱壳的方法与步骤。

1. 软件加壳

(1) 运行 ASPack 2.12,在其主界面选择“Open File”标签,从中单击【Open】按钮,如图 4-8 所示。

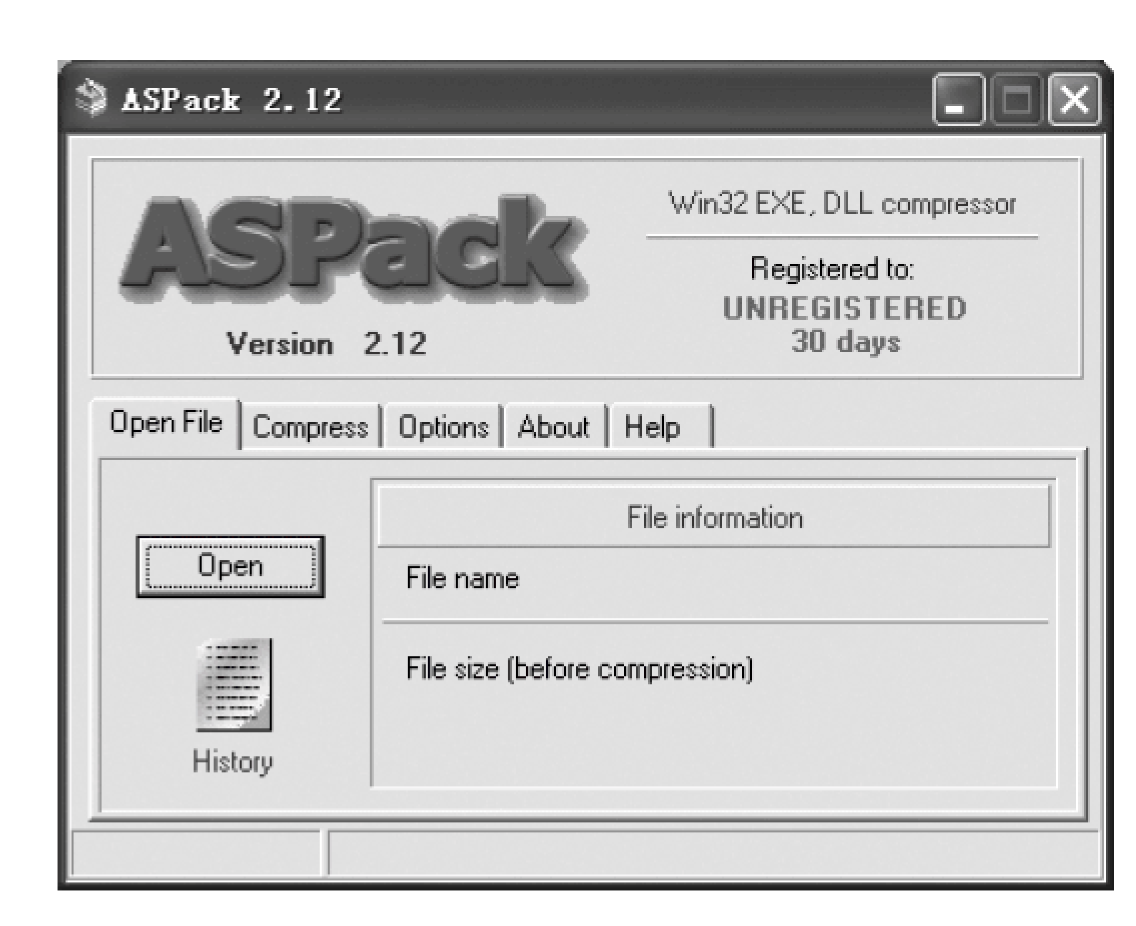


图 4-8 “ASPack 2.12”主界面

(2) 在打开的 Select file to compress 对

话框中选择要加壳的文件 ad4.402.installer.EXE(压缩前 2.11MB),然后单击【打开】按钮,如图 4-9 所示。

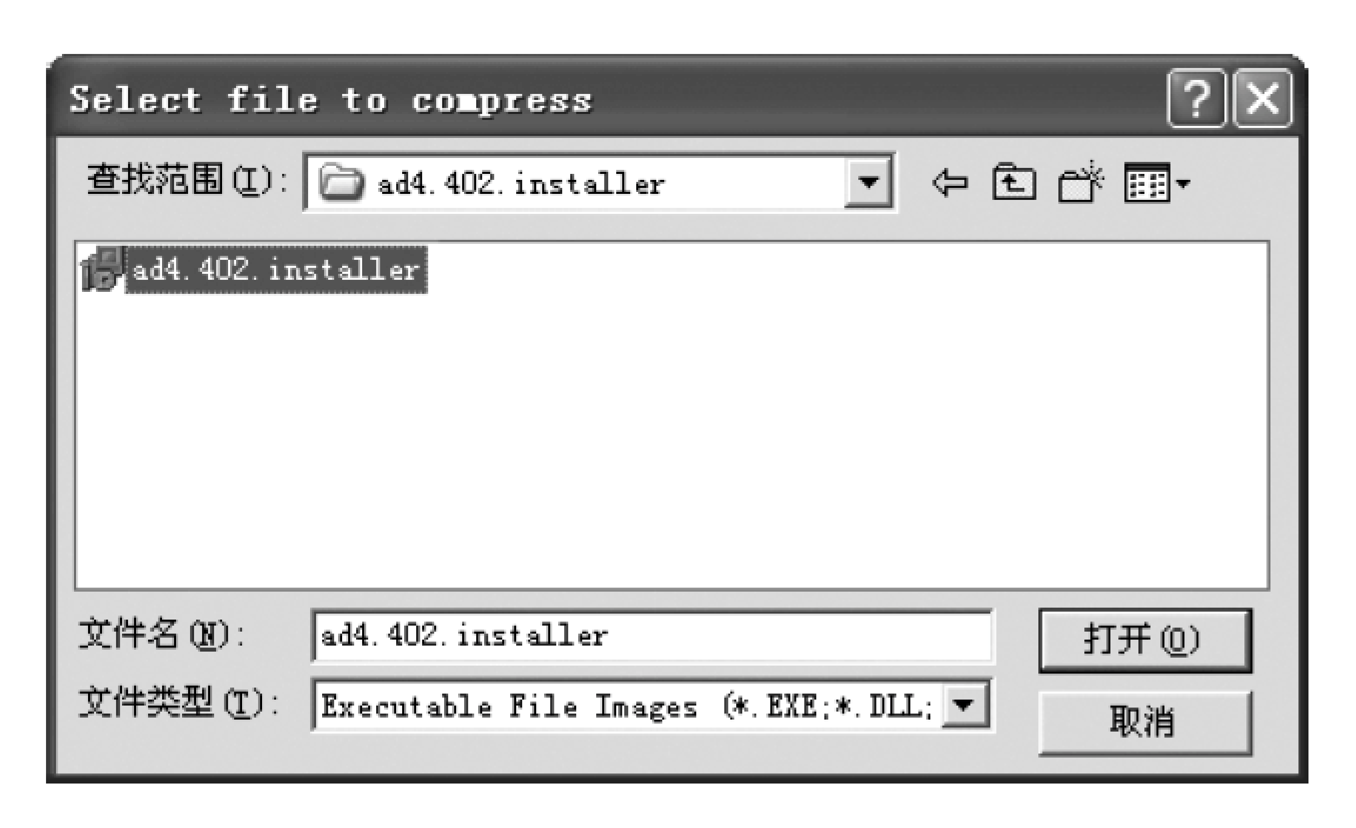


图 4-9　Select file to compress 对话框

接着可以看到软件会自动给 ad4.402.installer 加壳,如图 4-10 所示,并且很快就会自动加壳完毕。返回来查看 ad4.402.installer 文件,发现已经由原来的 2.11MB 压缩到了 37.8KB 了,可见 ASPack 对 ad4.402.installer 已进行了一次压缩壳。

2. 加壳类型侦测

假设此时并不知道 ad4.402.installer 是用什么软件加的壳。接下来可以用 Language 2000 来检测一下。

(1) 运行 Language 2000(中文版),在其主界面中单击【打开】按钮,如图 4-11 所示。

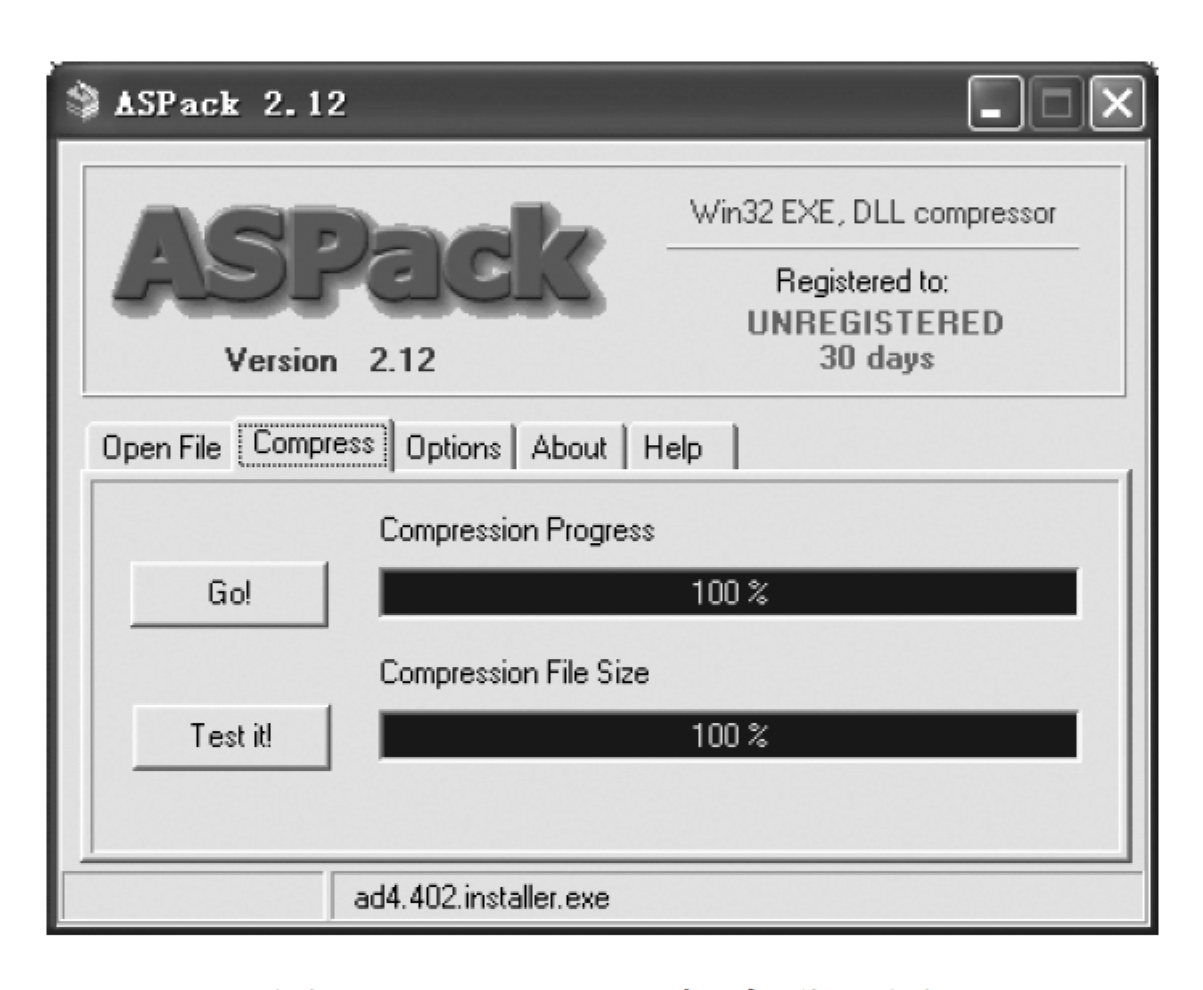


图 4-10　ASPack 加壳进程图



图 4-11　用 Language2000 侦测加壳类型结果显示界面

（2）在弹出的“浏览文件夹”对话框中，选择已经加了壳的 ad4.402.installer.EXE 文件，单击【确定】按钮后即显示探测结果，探测结果如图 4-11 所示。软件的版本、类型、编写软件等信息都显现出来了。其中“程序”一栏显示了加壳的类型，从这里就可以得到对方使用什么工具加壳的了。

3. 软件脱壳

当知道加壳的类型之后，就可以着手来脱壳了，在这里选用工具 ASPackDie 来完成。

（1）运行 ASPackDie1.41，打开“选择目标文件”对话框，如图 4-12 所示。



图 4-12 “选择目标文件”对话框

（2）选择 ad4.402.installer.EXE 文件后，单击【打开】按钮，解压后自动打开一个“ASPackDie-信息”对话框，提示脱壳后文件的名字和存放路径，如图 4-13 所示。



图 4-13 “ASPackDie-信息”对话框

（3）单击【确定】按钮后脱壳成功。接着查看 ad4.402.installer.EXE 文件发现又变回 2MB 多了。

以上使用 ASPack 2.12 加壳后脱壳的方法，每个软件的作者会选不同的脱壳工具，但基本操作的原理大同小异。

4.7.2 加密解密 WinRAR 压缩文件

WinRAR 是一款较 WinZip 推出晚一点的高效压缩软件，不但压缩比、操作方法都较

WinZip 优越，而且能兼容 ZIP 压缩文件，所以很快受到大家的青睐，现已成为人们常用的压缩软件，下面介绍通过 WinRAR 加密与解密的方法。

1. 用 WinRAR 加密文件

操作步骤如下：

（1）用鼠标右击需要压缩并加密的文件，在弹出的快捷菜单中选择“添加到压缩文件”命令。在打开的“压缩文件名和参数”对话框中，用户可以设置压缩文件的名称及压缩格式，如图 4-14 所示。

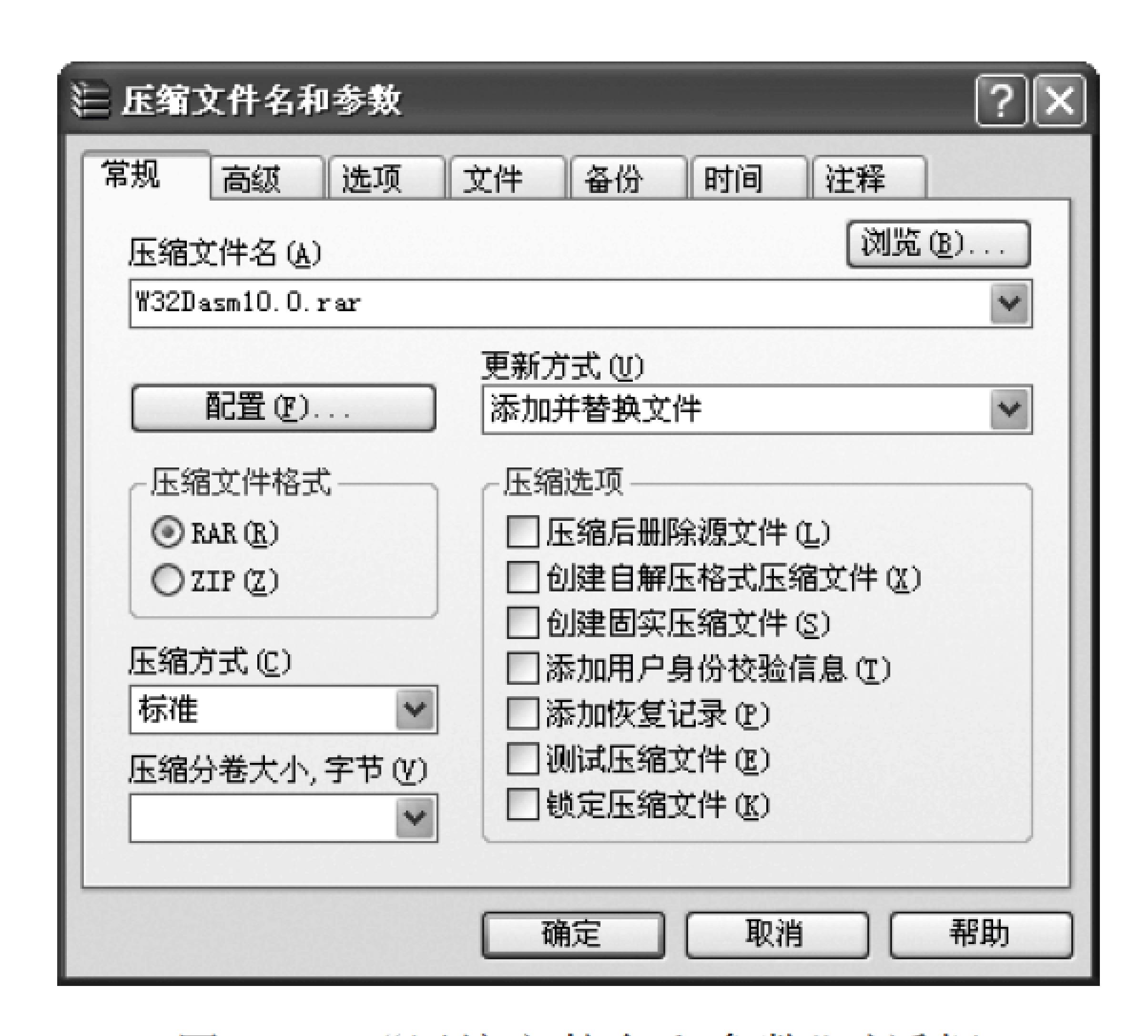


图 4-14　“压缩文件名和参数”对话框

（2）选择“高级”标签，从中单击【设置密码】按钮，如图 4-15 所示，在打开的“带密码压缩”对话框中，输入自己设置的密码，然后连续单击【确定】按钮即可生成加密的 RAR 文件。

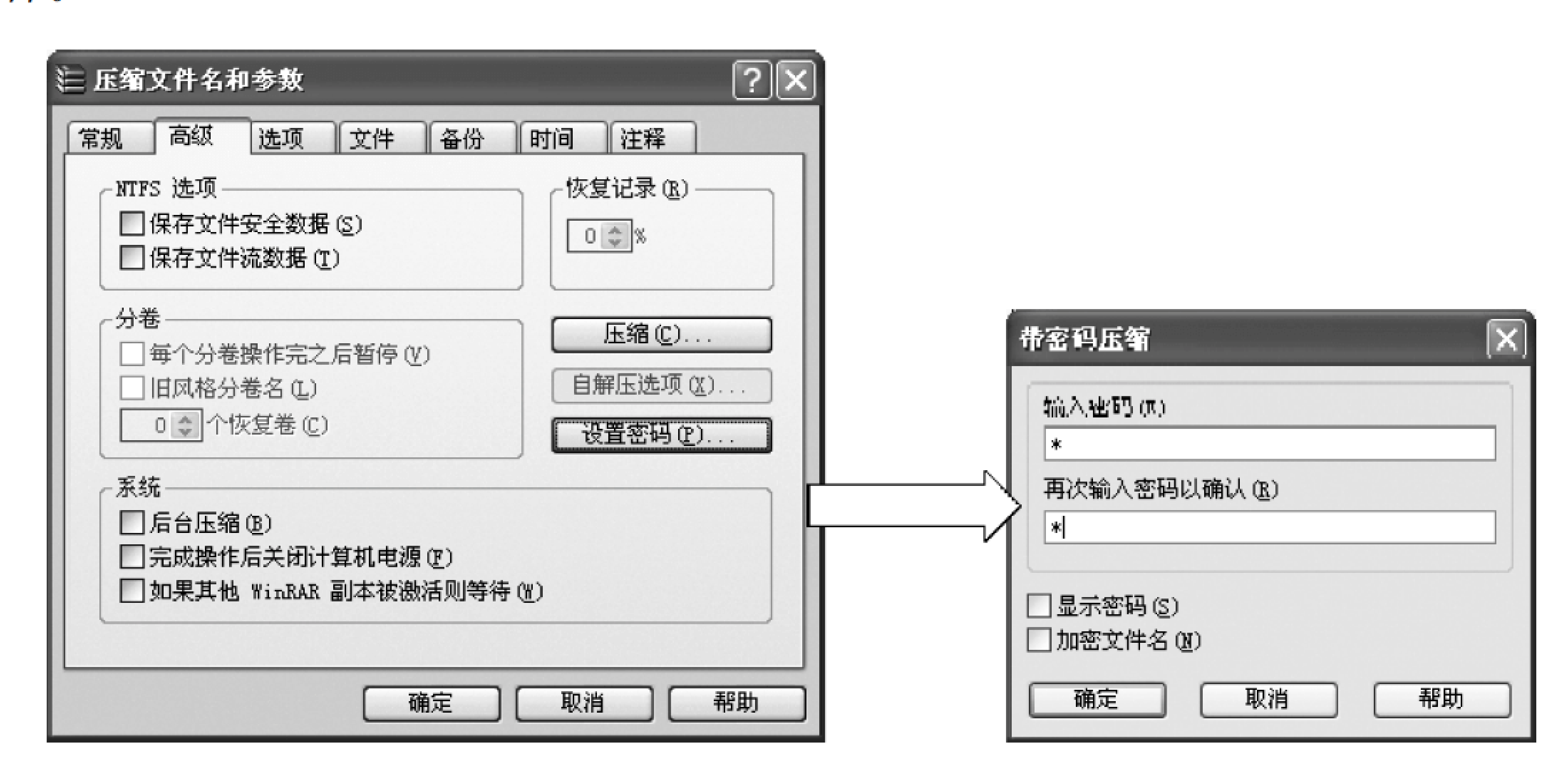


图 4-15　设置压缩文件密码示意图

2. 用 Advanced RAR Password Recovery 解密文件

Advanced RAR Password Recovery 是一款专门用于对 RAR 加密压缩文件进行解密的工具,其操作界面如图 4-16 所示。

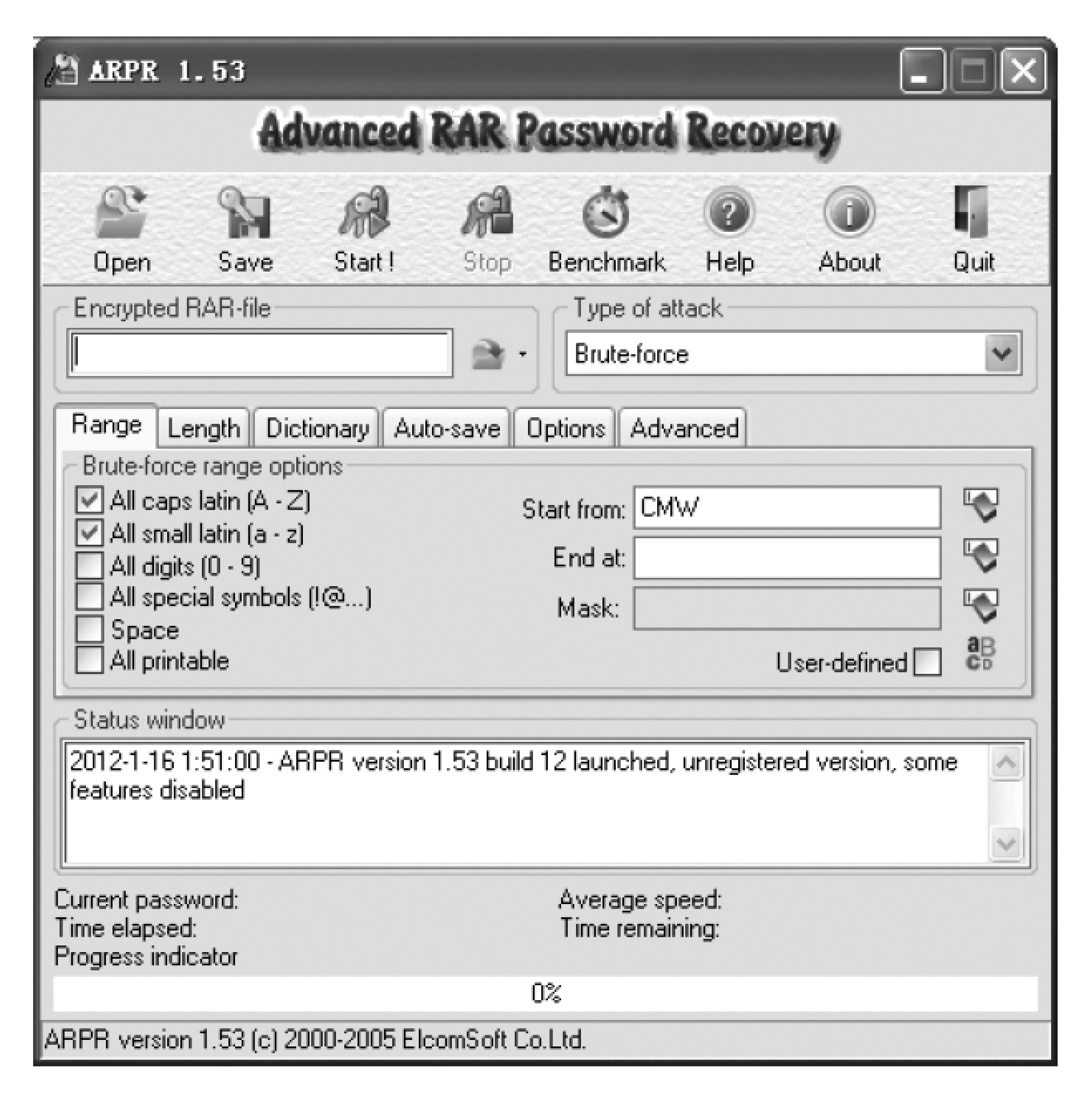


图 4-16　ARPR 1.53 操作界面

操作步骤如下:

(1) 单击“打开”按钮,在弹出的“打开”对话框中选取需要解密的 RAR 文件,单击【打开】按钮。

(2) 在 ARPR 1.53 主界面中单击【Start】按钮即可开始破解。破解成功后弹出“Password successfully recovered!”对话框,在“Total passwords”一栏显示了密码的信息,如图 4-17 所示。

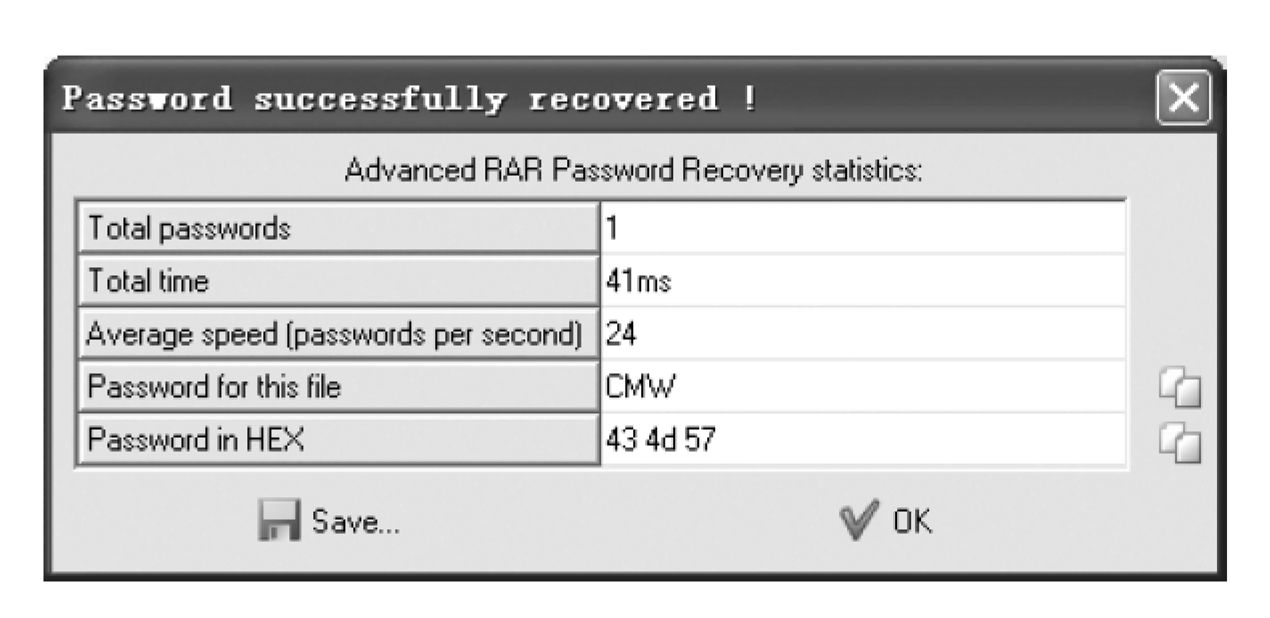


图 4-17　密码破解显示界面

3. 使用 RAR Key 解开 WinRAR 口令

RAR Key 软件是专门用于对 RAR 加密文档进行解密的工具,用 RAR Key 解密 RAR 文件的操作步骤如下:

（1）运行 RAR Key 软件，其主界面如图 4-18 所示。

（2）设置破解选项，在主界面单击【Settings】按钮，打开如图 4-19 所示的 Settings 对话框。

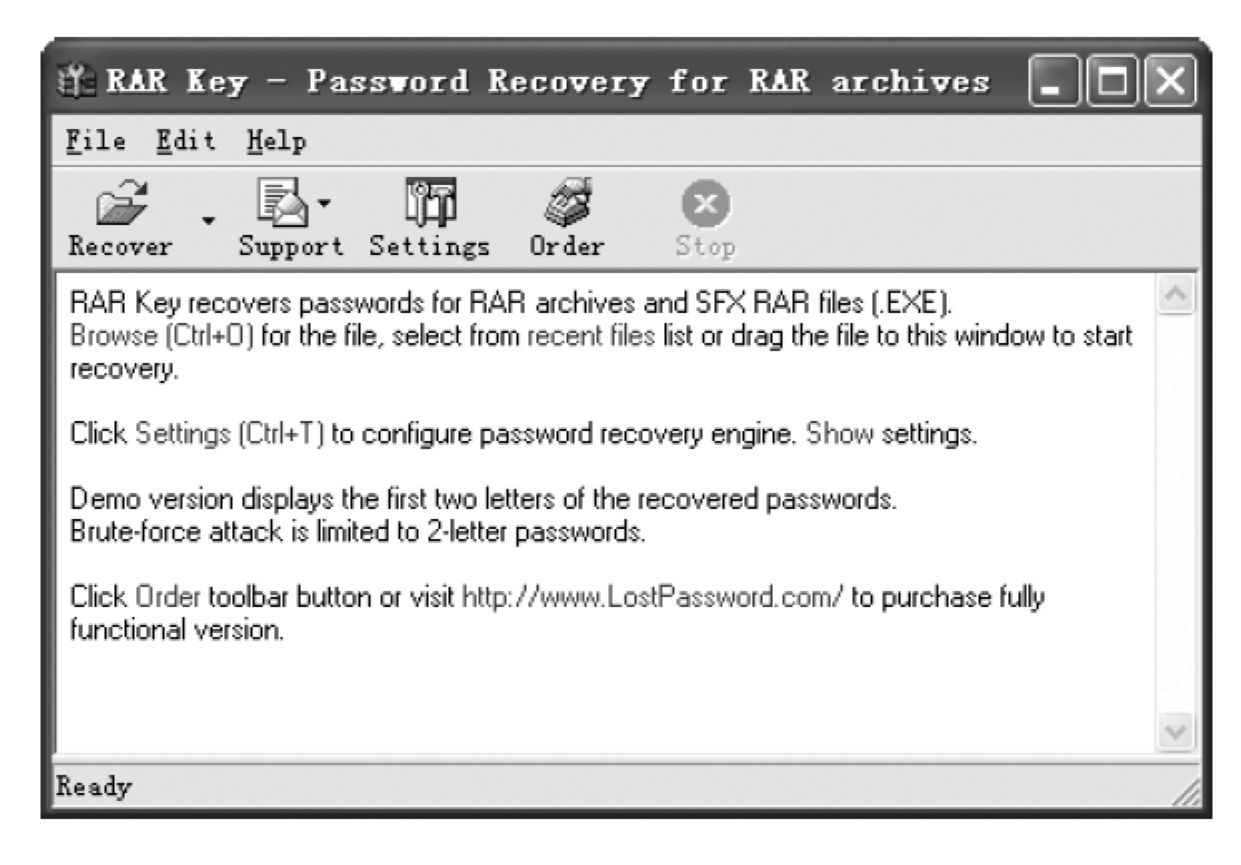


图 4-18　RAR Key 主界面

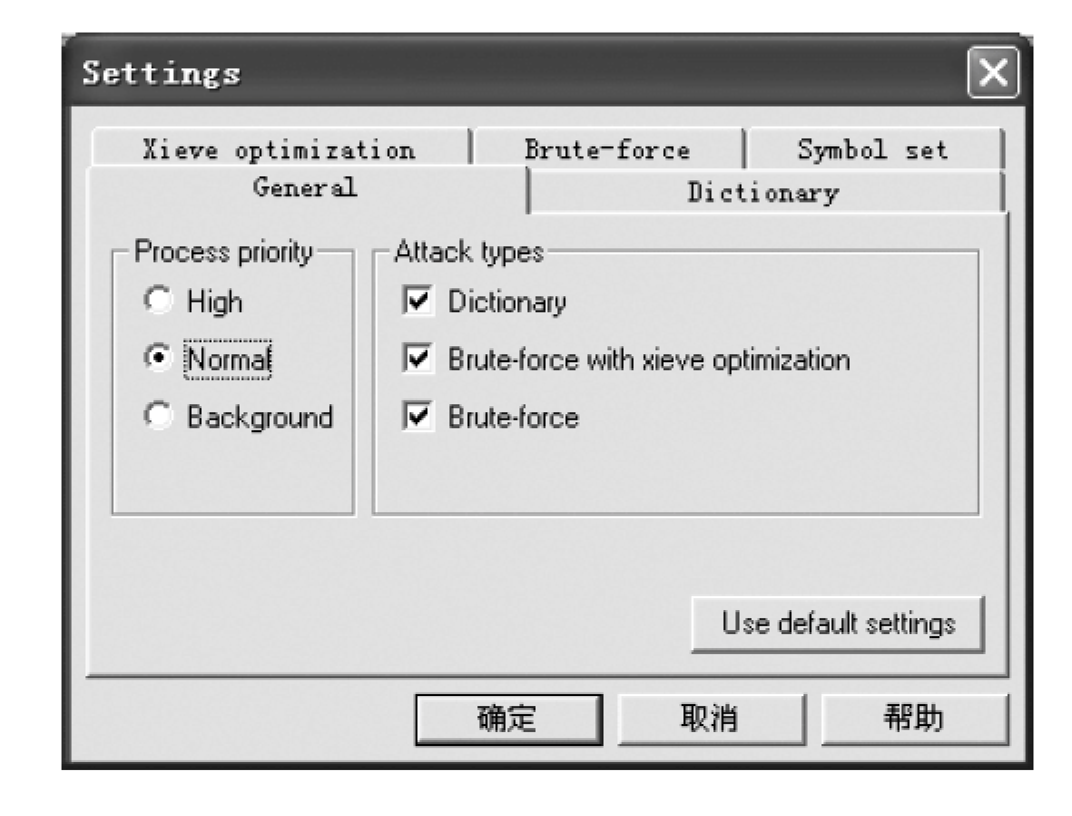


图 4-19　Settings 对话框

在“General”标签下，可以选择破解优先权和破解方式；在“Dictionary”标签下，可以选择是否使用字典文件破解、密码长度范围，同时还可以选择字典文件及组成密码的英文字母大写情况；在“Xieve optimization”标签下，可以选择是否使用优化暴力破解、优化暴力破解时密码的长度范围、执行优化暴力破解水平等选项；在“Brute-force”标签下，可以选择是否使用暴力破解方式以及破解时组成密码的长度。在“Symbol set”标签下，用户可以设置参与密码组合的各种字符。

（3）在 RAR Key 主界面单击【Recover】按钮，在打开的“Select file to recover”对话框中选择需要破解密码的压缩文件，单击【打开】按钮，如图 4-20 所示。



图 4-20　“选择解密文件”提示框

（4）单击【打开】按钮后即可按照用户设置好的条件进行破解。密码破解过程中显示的界面如图 4-21 所示，“Testing Password”显示了正在测试的密码，找到密码后，将给出

具体提示。

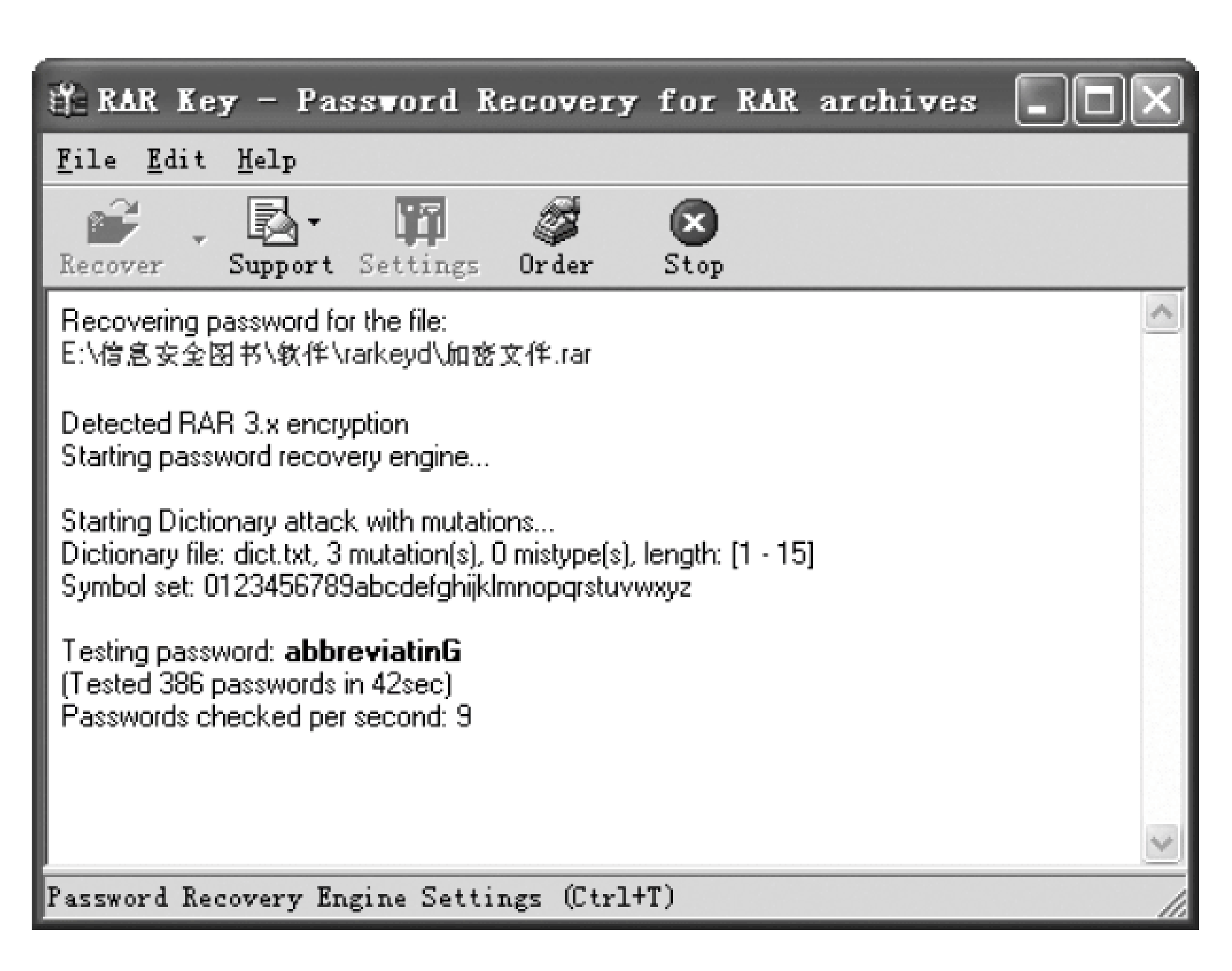


图 4-21 RAR Key 解密过程界面

4.7.3 加密解密 PDF 文件

PDF 是美国 Adobe 公司开发的一种通用文件格式，已成为在 Internet 上进行电子文档发行和数字化信息传播的理想文档格式。越来越多的电子图书、产品说明、公司文告、网络资料、电子邮件开始使用 PDF 格式文件。下面介绍一种 PDF 文件的加密解密方法。

1. 在 Adobe Acrobat 中加密 PDF 文件

为了保护文件的内容，Adobe 公司对 PDF 文件设置了一定的保护措施，但这一保护措施只能在 Adobe Acrobat 中实现，在 Adobe Reader PDF 阅读器中无法实现。

在 Adobe Acrobat 中，可以通过口令来限制用户打开、打印和编辑 Adobe PDF。如果已经签名或验证了文档，无法将口令加入到文档。有两类口令是可用的：

文档打开口令：在使用文档打开口令（也称为用户口令）的情况下，用户必须输入为打开 PDF 所指定的口令。

许可口令：当你仅设置一个许可口令（也称为主口令），用户不需要口令（用户口令）即可打开文档。但是，用户必须输入许可口令才能设置或更改受限功能。

如果用两种类型的口令保护 PDF，则它可用任一种口令打开。但是，只有许可口令才允许用户更改受限功能。

下面介绍 PDF 文件口令加密过程实现步骤。

第 1 步：打开 PDF 文件。

运行 Adobe Acrobat（以 Adobe Acrobat 9 为例），在主界面的菜单中选择“文件”→“打开”选项来打开一个 PDF 文件。

第 2 步：使用口令加密 PDF 文件。

（1）在菜单中选择“高级”→“安全性”→“显示安全属性”命令，打开如图 4-22 所示的“文档属性”对话框，在“安全性”标签下显示了当前 PDF 文件的安全设置，图中显示目前这个 PDF 文件无安全性设置，可以被任意处理。

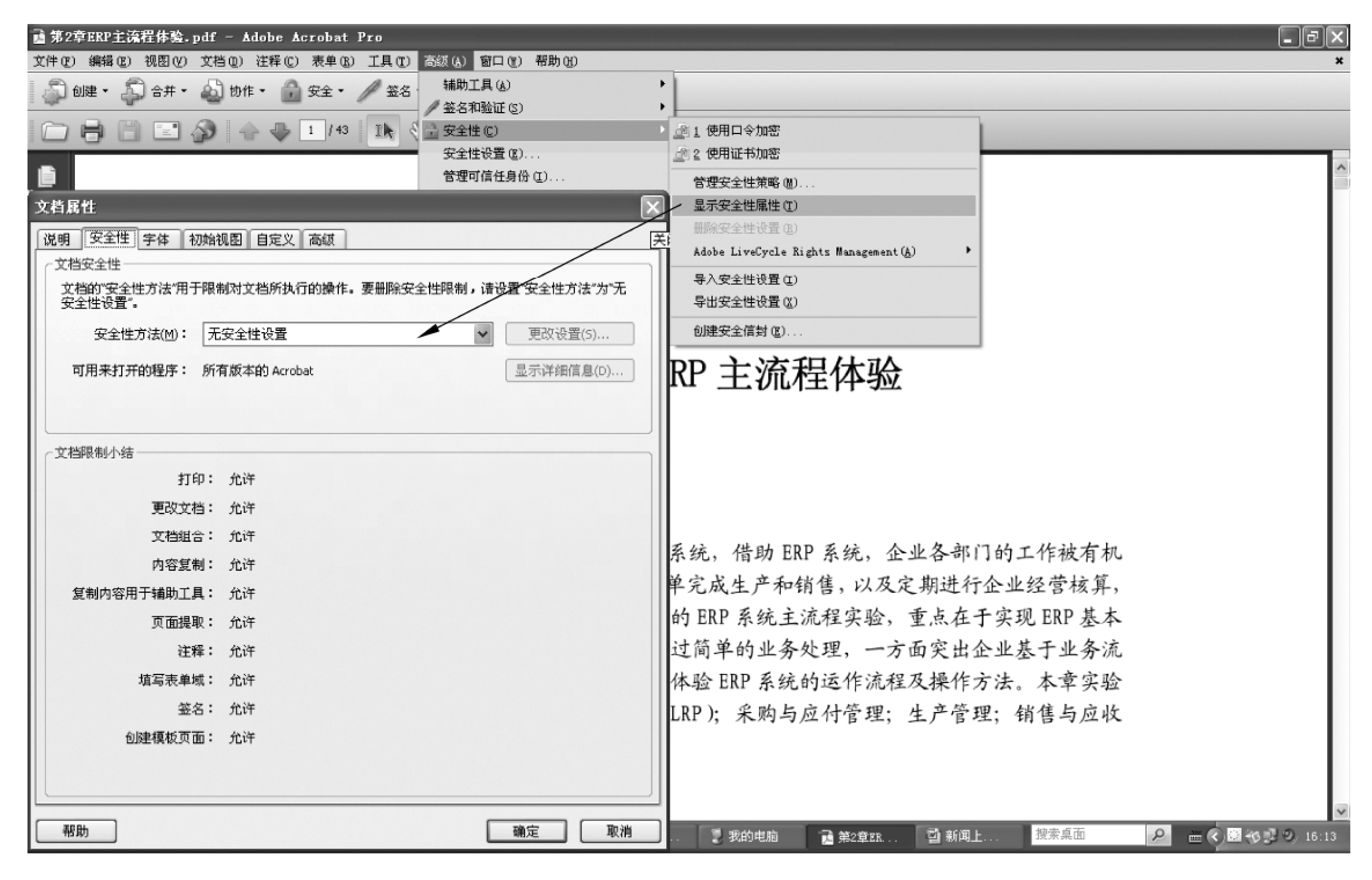


图 4-22 Acrobat 文档安全设置

(2)在菜单中选择“高级”→“安全性”→“使用口令加密”命令,打开“口令安全性-设置”对话框,如图 4-23 所示。



图 4-23 “口令安全性-设置”对话框

(3) 在“口令安全性-设置”对话框中勾选“要求打开文档的口令”，然后输入打开文档口令，这样用户在打开该 PDF 文档时，就必须输入口令；在“许可”框中勾选“限制文档编辑和打印。改变这些许可设置需要口令”，然后输入更改许可口令，这样在修改文档和口令时要求输入该口令；可以在“许可”框中设置“允许打印”项，指定允许用户用于 PDF 文档的打印级别；设置“允许更改”项，定义允许在 PDF 文档中执行的编辑操作，如图 4-23 所示。

(4) 所有这些操作完成后，保存文件。此时再在“文档属性”对话框中的“安全性”标签项中单击【显示详细信息】按钮，打开“文档安全性”对话框，显示文件的安全性设置如图 4-24 所示，表示该文件已被加密。

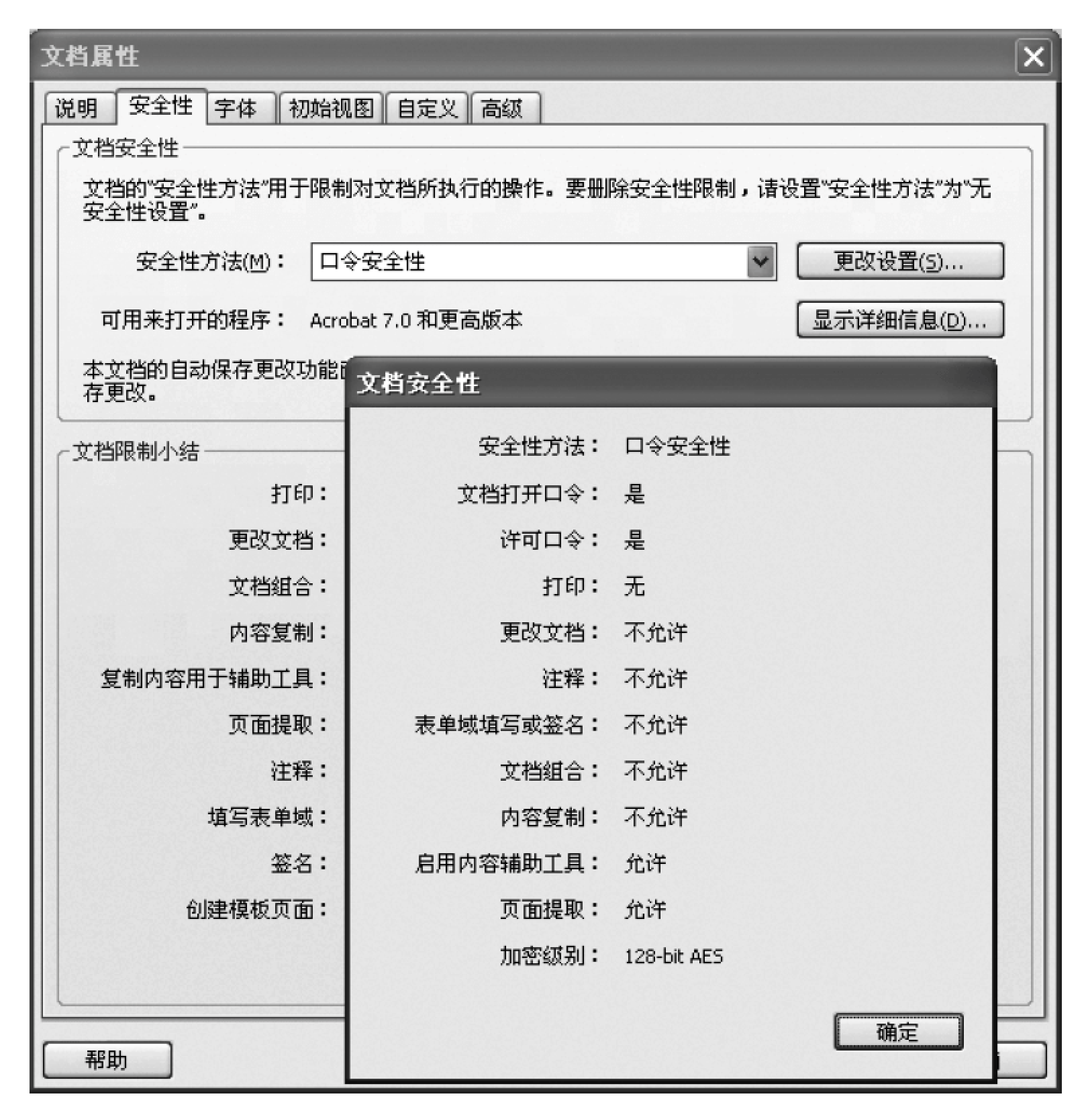


图 4-24　显示文档安全性信息

(5) 再次打开该 PDF 文档时会弹出“口令”对话框，提示输入口令，如图 4-25 所示。

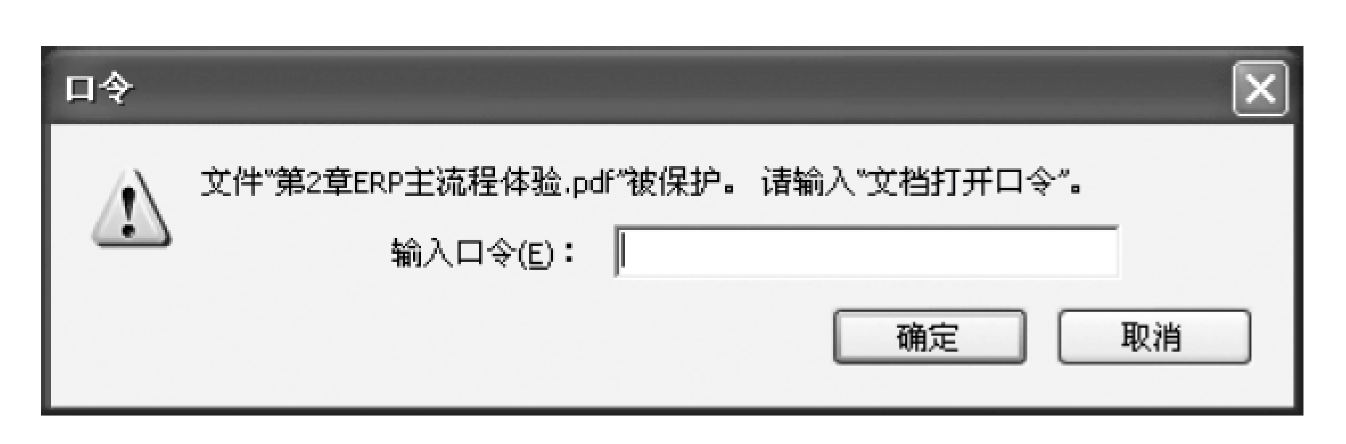


图 4-25　“口令”对话框

2. 利用 Advanced PDF Password Recovery 破解 PDF 加密文件

Advanced PDF Password Recovery（简称 APPR）是一款专门用来解密受保护的 Adobe Acrobat PDF 文件的工具软件，它能方便地去除 PDF 文件内在的保护。该软件的安装方法很简单，就不再赘述。破解操作步骤如下。

（1）APPR 安装完成后，启动该程序，打开如图 4-26 所示的 Advanced PDF Password Recovery 操作界面。

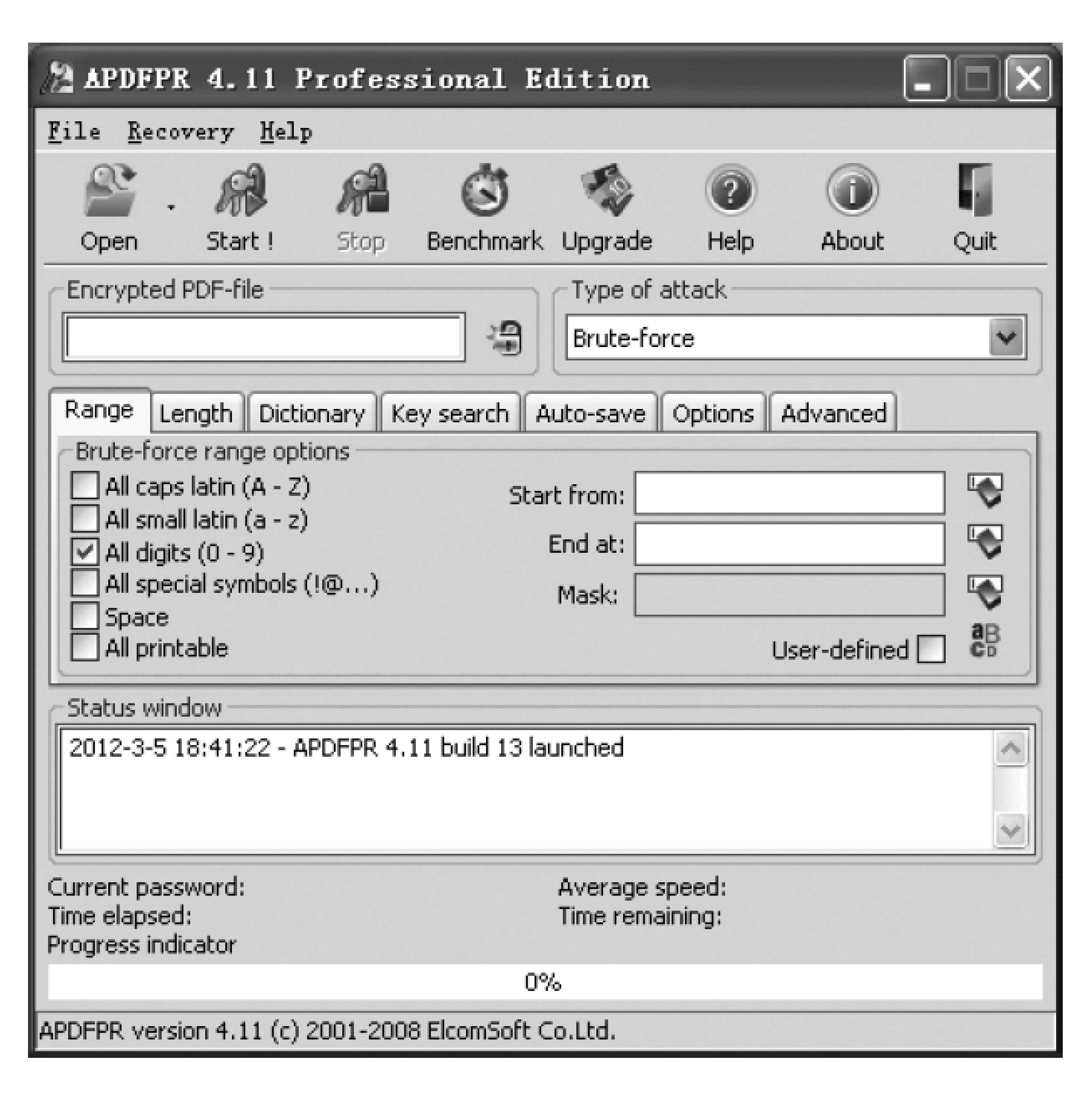


图 4-26　Advanced PDF Password Recovery 操作界面

（2）单击“Open”按钮，在打开的“Open”对话框中选择需要解密的 PDF 文件，然后单击【Open】按钮。

（3）在文件解密前需要设置一些基本选项。在“Type of attack”下拉列表框中，用户可以选择“Brute-force”（暴力攻击）、“Mask”、（掩码）、“Dictionary”（字典文件）、“Key search”（密码搜寻）等破解方式。

（4）在“Range”标签中，用户可以设置暴力攻击的范围；在“Length”标签中可以设置密码长度的范围；在“Dictionary”标签中，用户可以选择破解时所使用的字典文件；在“Key search”标签中，用户可以设置密码搜寻的范围；在“Auto-save”标签中，用户可以设置自动保存的时间间隔、保存的文件名及文件夹；在“Options”标签中，用户可以设置使用该软件时的各种选项。

（5）设置好各种选项后，单击“Start!”按钮，即可按用户设置的选项开始破解，并给出最终提示，如图 4-27 所示。

（6）在 APPR 的操作界面中，单击“Decrypt now”按钮可将去除密码后的 PDF 文件直接以一个新的文件名保存到用户指定的文件夹中。

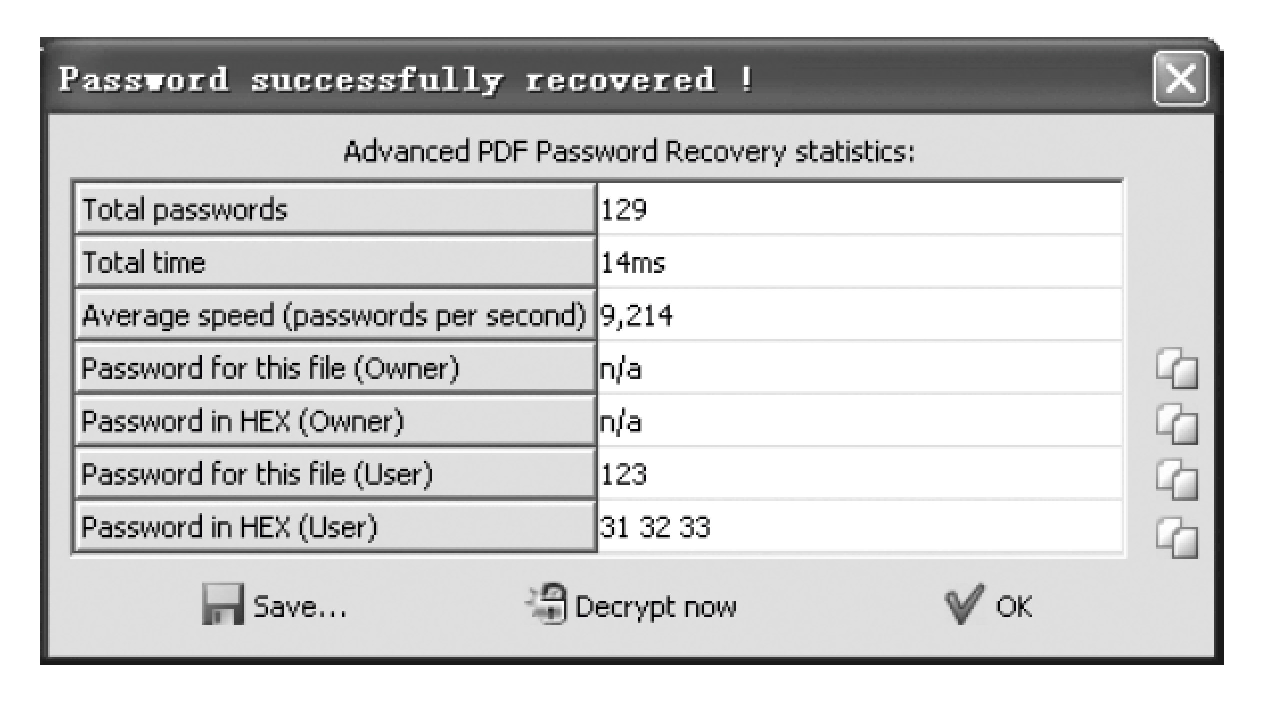


图 4-27　密码被成功破解

4.7.4　加密解密 Excel 文件

Excel 是 Microsoft Office 套件中的一个重要的组成部分，其功能强大，操作简单，应用十分广泛。那么如何才能保护自己的电子表格，使别人不能打开，或允许其打开后不能修改呢？下面就来介绍 Excel 文档的一些加密解密方法。

1. 通过 Excel 自身功能加密

Excel 本身就具有设置密码的功能，以 Microsoft office Excel 2007 为例介绍其操作方法如下。

第 1 步：为 Excel 设置文档打开密码。

(1) 打开一个编辑好的电子表格，单击左上角的 office 图标，在弹出的下拉菜单中选择“准备”→“加密文档”菜单命令，打开“加密文档”对话框，如图 4-28 所示。



图 4-28　打开“加密文档”对话框

(2) 在打开的“加密文档”对话框中输入打开电子表格的密码,然后单击【确定】按钮,如图 4-29 所示。在弹出的“确定密码”对话框中再次输入设置的打开密码,然后单击【确定】按钮,即设置文档打开密码完成,其他用户在打开该表格时就必须输入正确的密码才能打开。

第 2 步:为 Excel 工作表设置保护密码。

(1) 在工具栏的“审阅”功能区下,单击【保护工作表】按钮,打开“保护工作表”对话框,如图 4-30 所示。

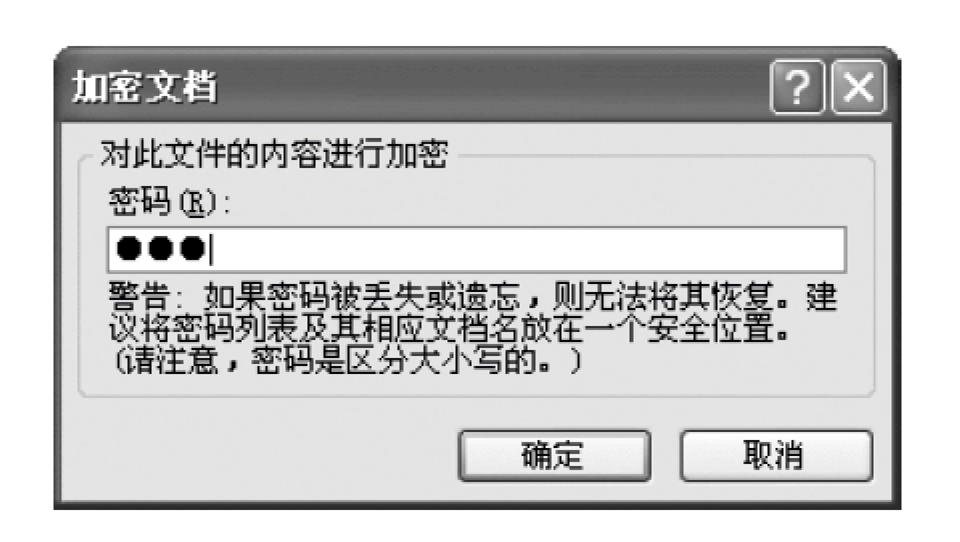


图 4-29 “加密文档”对话框

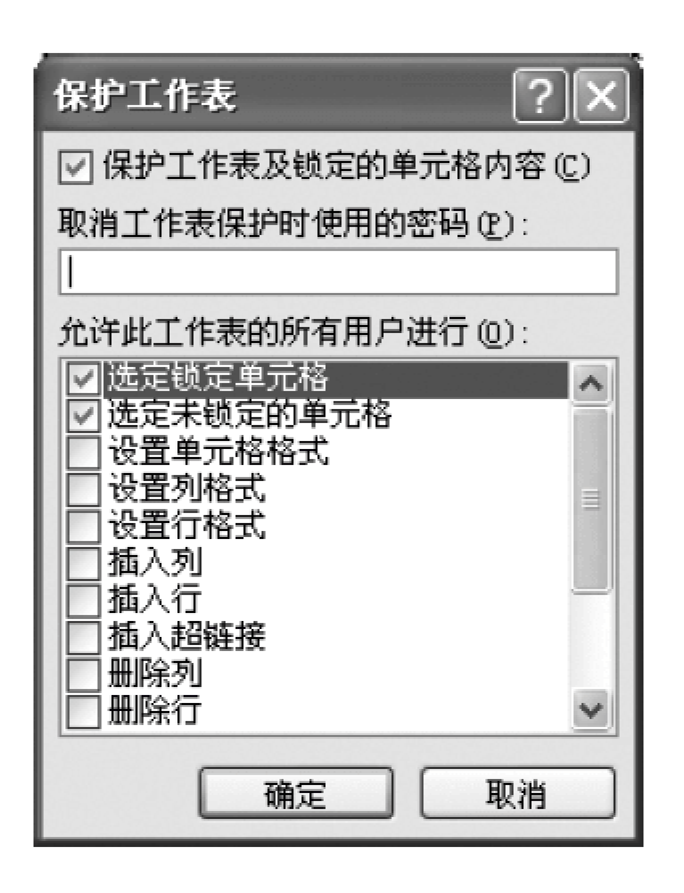


图 4-30 “保护工作表”对话框

(2) 在“取消工作表保护时使用的密码”文本框中输入自己的密码,在“允许此工作表的所有用户进行”列表框中选择允许其他用户可以操作的选项,即打“√”复选框表示允许其他用户进行此项操作,否则不能进行此项操作。单击【确定】按钮即可设置完毕。此后当前表格中的内容只允许浏览不允许修改。

(3) 如果想修改此表格,则可在“审阅”功能区下,单击【撤销工作表保护】按钮,在打开的【撤销工作表保护】对话框中输入先前设置的密码,单击【确定】按钮取消对工作表的保护,如图 4-31 所示。

第 3 步:为 Excel 工作簿设置保护密码。

(1) 在工具栏的“审阅”功能区下,单击【保护工作簿】按钮,在弹出的下拉列表中选择【保护结构和窗口】,弹出“保护结构和窗口”对话框,如图 4-32 所示。



图 4-31 “撤销工作表保护”对话框

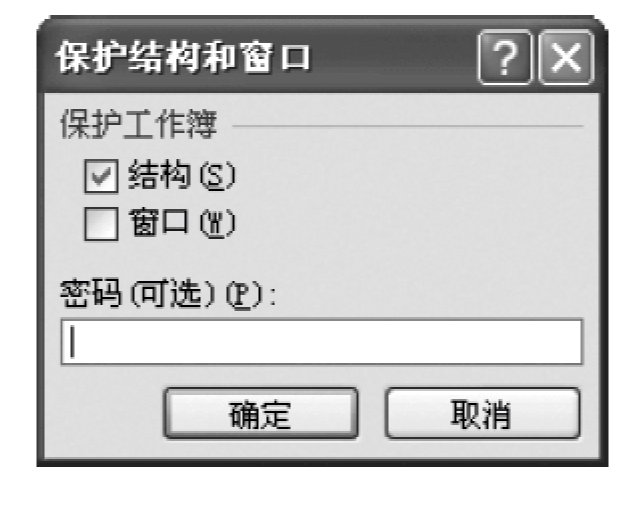


图 4-32 “保护结构和窗口”对话框

(2) 用户在该对话框中可以输入自己的密码,并选取保护工作簿的范围(即结构和窗口),单击【确定】按钮,这样就可以防止其他用户添加和删除工作表,或是显示隐藏的工作表。同时还可以防止用户更改已设置的工作簿显示窗口的大小或位置。

(3) 如果想取消对工作簿的保护,则需在再次单击【保护工作簿】按钮,在下拉列表中选择【保护结构和窗口】,此时弹出"撤销工作簿保护"对话框,如图 4-33 所示。在显示的"密码"文本框中输入原来设置的密码,单击【确定】按钮撤销对工作簿的保护。



图 4-33 "撤销工作簿保护"对话框

2. 利用 Advanced Office Password Recovery 破解 Excel 文件打开密码

Advanced Office Password Recovery(简称 AOPR)是一个多功能 Office 文档密码破解工具,能够处理微软公司的各种常见文档格式,涵盖从 Word 到 Project 在内的 14 种类型。本文以 Advanced Office Password Recovery 4.15 为例介绍利用该软件破解 Excel 文档打开密码的操作步骤。

(1) 运行 AOPR 4.15,其操作界面如图 4-34 所示。AOPR 与上一小节介绍的 PDF 破解工具 APPR 的使用方法类似,其选项设置在此就不赘述。

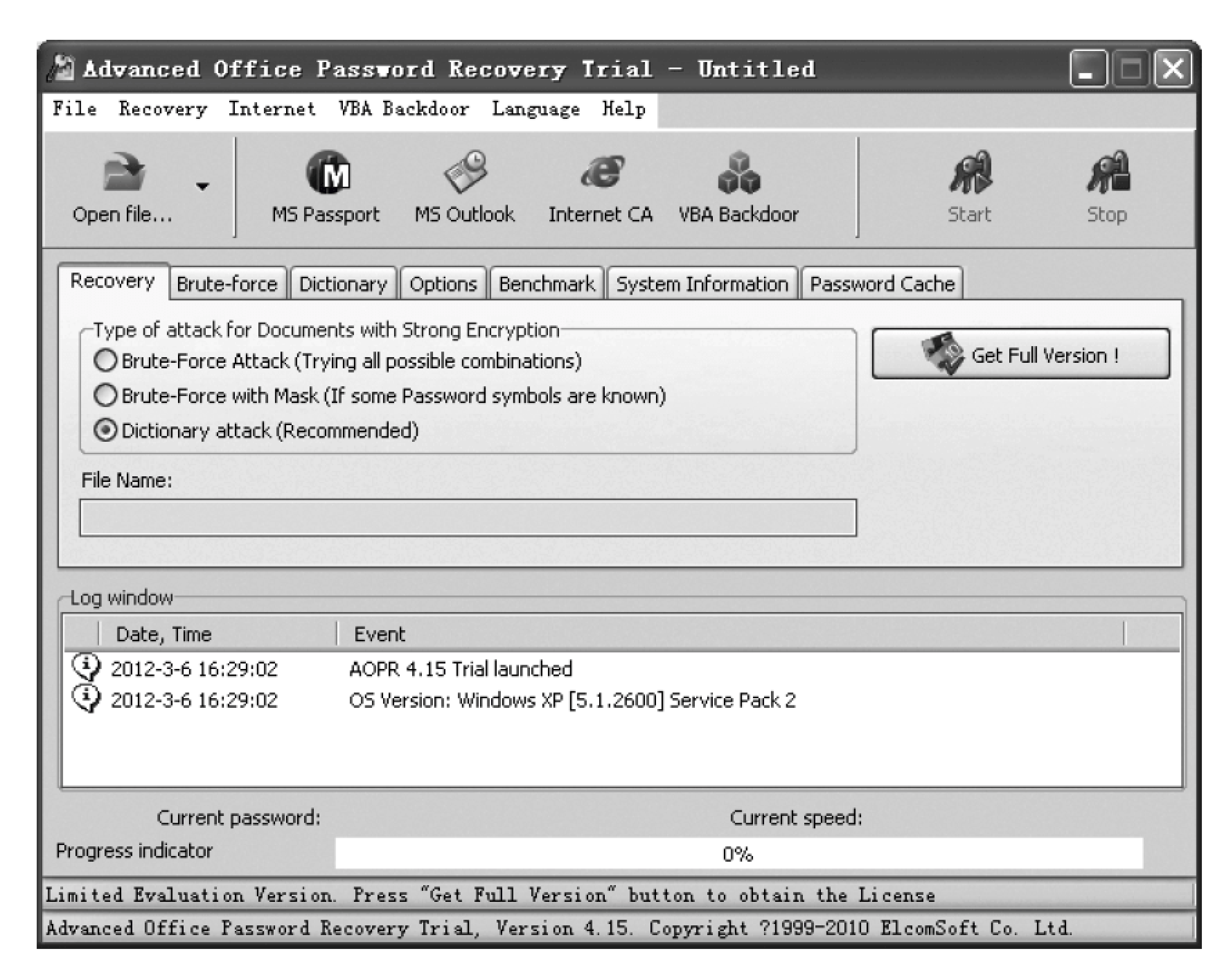


图 4-34 AOPR 4.15 操作界面

(2) 设置好各种选项后,单击"Open file"按钮,在弹出的"Open File"对话框中选择需要破解密码的 Excel 文件,单击【Open file】按钮,软件就自动开始破解密码。密码破解成功后弹出提示框"Excel Passwords Recovered",并给出破解出的 Excel 文档密码信息,如图 4-35 所示。

3. 利用 Excel 密码工具箱软件解除 Excel 工作表、工作簿的密码保护

Excel 密码工具箱是一款增强型插件,用于解除工作簿密码,解除工作表密码,解除 VBA 密码,解除 IE 上网密码,工作表批量加密码,工作表批量解密码。在此介绍其解除

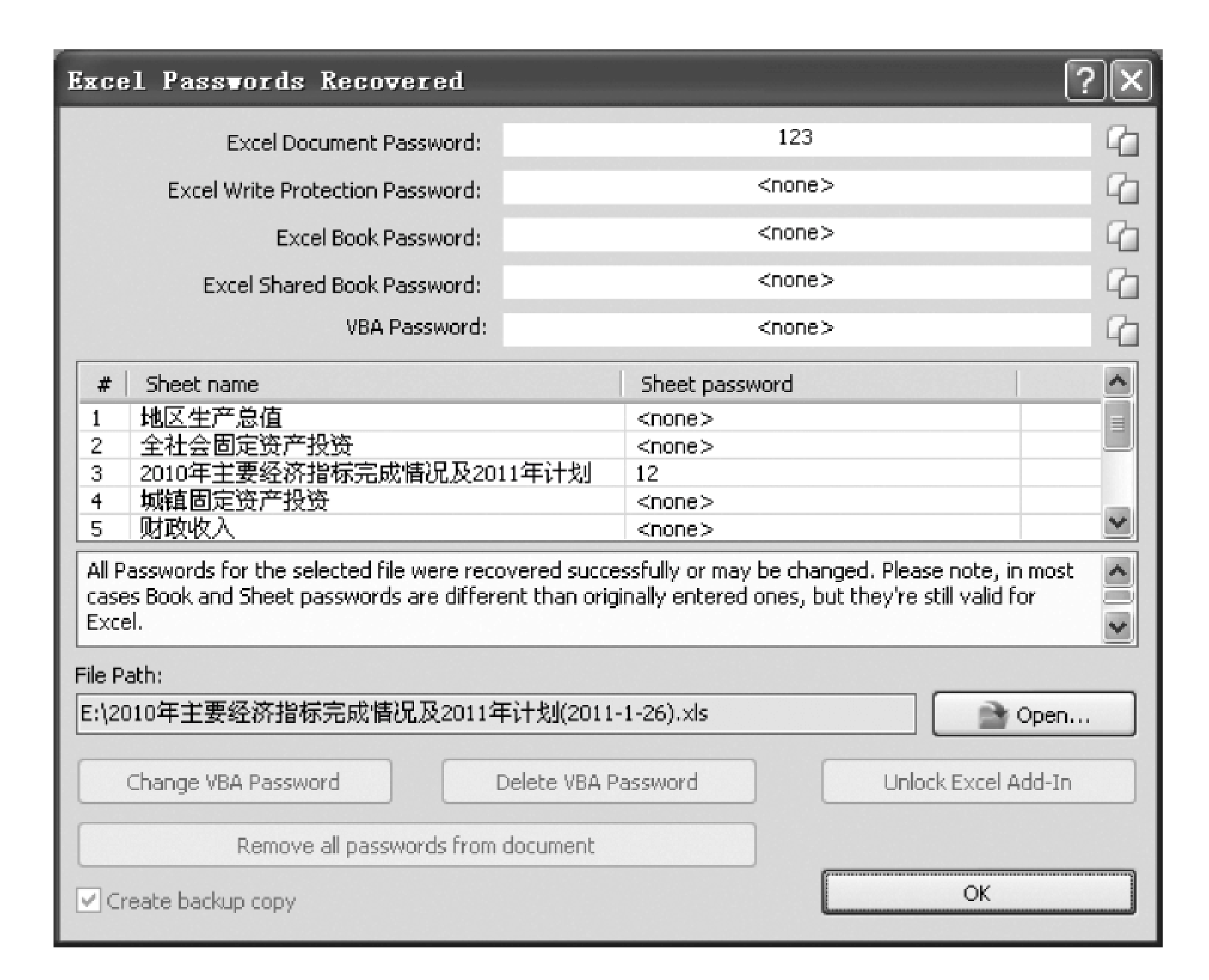


图 4-35　Excel Passwords Recovered 窗口

工作表和工作簿密码的步骤。

（1）到网上下载并安装 Excel 密码工具箱，安装之前要先关闭所有的 Excel 文档。安装完毕后，打开 Excel 文档，发现在菜单栏的“开始”标签右侧增加了一个“解密工具”标签。单击“解密工具”标签，显示的标签页内容如图 4-36 所示。



图 4-36　“解密工具”标签



图 4-37　“撤销工作表保护”按钮

（2）在工具栏“审阅”标签下，加了保护工作表密码的【保护工作表】会变成【撤销工作表保护】按钮，如图 4-37 所示。如果不知道密码但要撤销工作表的保护，可以单击“解密工具”标签下的【工作标记密码】按钮，弹出“百宝箱之密码攻略”对话框，单击【确定】按钮，如图 4-38 所示。在打开的“撤销工作表保护”对话框中按之前的提示单击【取消】按钮，如图 4-39 所示。此时“审阅”标签下又变回了【保护工作表】按钮，表示密码保护已被解除。



图 4-38　“百宝箱之密码攻略”对话框



图 4-39　“撤销工作表保护”对话框

(3) 同理，要想解除工作簿的密码保护，可以单击“解密工具”标签下的【工作簿密码】按钮，稍等片刻会弹出解密成功的“友情提示框”，单击【确定】按钮。此时工作簿的密码保护已被解除，又可以在工作簿中添加、删除和显示隐藏的工作表了。

4.8 案例讨论

案例 4-1 手机软件漏洞

2011 年年底，360 安全中心监测发现，360 手机精灵 1.3.0 版本、QQ 应用助手 beat3、豌豆荚守护精灵 1.24.12.9 版本等手机应用软件，在公共 Wi-Fi 局域网环境下存在一个访问权限漏洞。在某些特殊条件下，该漏洞有可能被黑客利用来获取手机信息。

360 手机精灵、QQ 应用助手、豌豆荚守护精灵是用于手机与计算机同步的软件，用户在手机上安装上述软件后，可以把手机连到计算机上以同步数据。但上述软件在设计上都存在一个缺陷，即没有严格限制手机只能连接用户个人指定的计算机，导致在手机 Wi-Fi 打开情况下，有可能遭到来自同一公共 Wi-Fi 局域网内的黑客攻击，在某些特殊条件下存在泄露手机信息的可能。

发现这一问题后，360 技术人员立即修复了 360 手机精灵老版本的漏洞。目前，用户可以将手机与安装了 360 手机助手的计算机连接，连接后手机精灵会自动升级到已修复的安全版本 1.3.1。

此外，360 安全中心已将该漏洞上报国家漏洞库及相关部门，并向腾讯和豌豆荚两家公司进行了通报，建议他们尽快修复各自产品的漏洞，并愿为其提供相应的技术支持。

360 安全专家石晓虹博士表示：目前上述软件都只有安卓版本，用户量都不大，并且该漏洞攻击不能在互联网上远程进行，只能在同一公共 Wi-Fi 局域网上近距离实施，而且需要一些特殊条件，因此实际上被黑客利用的概率很小。在升级到最新的安全版本后，用户可以继续放心使用此类软件。

讨论“访问权限漏洞”可能是怎么产生的，有哪些软件漏洞监测和修复方法？

案例 4-2 PS3 被破解

2011 年 2 月，索尼在 PS3(PlayStation3，索尼电脑娱乐所开发的第三款家用游戏机)连遭一系列破解事件后，对涉嫌破解 PS3 的一些黑客提起了诉讼，指控他们违反了《数字千年版权法》和《计算机欺诈和滥用法》，并且实施了各种侵犯版权和违反二进制技术规范的行为。对此，被起诉的黑客们迅速作出回应，声称自己是合法的。专家表示，由于根键位于 PS3 硬件系统的最核心位置，因此一旦被破解，很难修补。

此次被索尼诉讼的被告包括别名“Geohot”美国知名黑客乔治(George Hotz)、黑客团体 failoverflow，以及一些未被透露姓名的黑客。霍兹之前成功解锁了苹果 iPhone，此次他用类似的方法提取了 PS3 主密钥，并在互联网上公开。failoverflow 黑客团体还发布

了一系列破解工具，索尼表示，这些破解工具攻破了 PS3 的保护措施，使得盗版软件有机可乘。索尼请求法院下达临时禁令，要求撤下网上的所有破解工具，并查封霍兹的个人电脑和其他相关媒体。目前，霍兹的网站 Geohot. com 已经被关闭。

对于索尼的控诉，乔治在接受采访时为自己辩解："我是一个数字知识产权的坚定拥护者，我期望看到一家有着知识产权的公司本身能有良好的法律意识。但是索尼目前的行动让我感动失望。我曾经与律师交谈过并且结果令我感到欣慰，那就是索尼这样的行为完全没有法律依据。"

被起诉的黑客成员还有一个名为 failoverflow 的黑客团队，他们也否认自己有任何不当行为。该组织通过雅虎发布了一份联合声明，并声称自己从未纵容、支持、批准或鼓励盗版视频游戏。

不过索尼对他们的辩解显得不屑一顾，索尼称他们尽管口中说着并未支持盗版，但他们的工作却会导致这个事情发生，现在如果不加以制止，那么未来将对索尼产生无法弥补的伤害。

美国媒体报道，为了和索尼打官司，霍兹已经倾家荡产，只能通过网上募捐的方式来支持诉讼。2011 年 4 月，为了躲避追捕，逃亡南美的霍兹终于与索尼达成和解。但是，和解协议被媒体曝光，协议中霍兹保证不再针对索尼主机从事破解活动，后者则答应就此罢手不再追究。虽然看上去不分胜负，但实际上双方对这个结果都不满意，索尼的打击破解活动并未取得计划的成效，而霍兹则生气地表示从此再不买索尼的任何产品。

你如何看待手机或游戏机的"越狱"行为？"越狱"给软件安全又带来了哪些威胁？

归纳总结

1. 根据本章内容，总结可以运用哪些软件安全防护技术来防止软件盗版。
2. 归纳总结在个人使用软件过程中应该使用什么保护方法。
3. 你目前会使用什么软件保护技术？归纳总结你应该掌握哪些软件安全技术。

思考与实践

思考题

1. 保障计算机软件安全的技术有哪些？它们各自又有什么用途？
2. 为什么要保证计算机软件的安全？
3. 什么是软件加密技术，它有哪些分类？
4. 什么是壳？如何给软件进行加壳和脱壳？
5. 什么是反动态跟踪技术？它有什么作用？

6. 什么是软件限制技术？思考你遇到过哪些软件限制？

实践题

1. 上网了解除课本介绍之外的其他软件保护技术。

2. 上网了解市场上有哪些加密狗软件,并尝试安装使用一种加密狗软件,了解其如何对软件进行保护。

3. 尝试安装使用多种加壳脱壳工具,并比较这些工具的异同。



第5章 系统软件安全技术

学习目标

通过本章的学习,能够——

- 了解系统软件的概念;
- 了解系统软件面临的安全威胁;
- 知道如何进行系统软件安全设置;
- 知道如何进行系统软件安全管理。

引导案例

2007年5月18日,在操作系统中安装了诺顿杀毒软件的用户,将诺顿升级最新病毒库后,诺顿应用软件会把Windows XP操作系统的关键系统文件netapi32.dll、lsasrv.dll隔离清除,当计算机重启后操作系统软件将会瘫痪。操作系统软件是最底层的软件,它控制所有计算机运行的程序并管理整个计算机的资源,是计算机裸机与应用程序及用户之间的桥梁,没有它,用户也就无法使用某种软件或程序。因为诺顿这次病毒库升级的有误操作,根据瑞星公司统计,截至2007年5月18日中午12点已有超过7千名个人用户和近百家企业用户向瑞星客户服务中心求助,更多用户由于系统繁忙无法打入电话,在当时中国大陆地区有数百万台计算机面临崩溃的危险。

武汉的付强是深圳某信息公司武汉办事处工程师,曾为省交警总队开发车辆驾驶管理信息程序。2007年起,他使用一种软件查询数据库获取数据库用户表,然后用自己"超级管理员"的身份,用超级密码登录省交警总队数据库,入侵省交警总队车管数据库系统,为走私车办理牌照。这个"地下车管所",先后为126辆高档走私汽车办理假证号牌,非法获利1500余万元。

可见数据库系统作为一个信息的聚集体,其安全的不足不仅会损害数据库本身,而且还会引起经济、制度等一系列的安全问题。

5.1 系统软件安全概述

和第 4 章中的软件有所区别，本章主要介绍的是系统软件，仅指操作系统软件与数据库软件，它们具有软件安全的共性，本章要介绍它们在安全方面的特性。

本节主要介绍系统软件的含义、面临的安全威胁、安全体系结构与安全技术。

5.1.1 什么是系统软件

系统软件主要指面向硬件或者开发者所设立的软件，它们用来控制和协调计算机及外部设备，支持应用软件开发和运行，它是无需用户干预的各种程序的集合，其主要功能是调度、监控和维护计算机系统，负责管理计算机系统中各种独立的硬件，使它们可以协调工作，如操作系统、解释系统、编译系统，数据库系统、中间件等面开发者的软件。本章重点介绍系统软件中操作系统和数据库系统两大类系统软件的安全技术。

1. 操作系统

操作系统是计算机系统的控制和管理中心，从资源角度来看，它具有处理机、存储器管理、设备管理、文件管理 4 项功能。大致包括 5 个方面的管理功能：进程与处理机管理、作业管理、存储管理、设备管理、文件管理。以现代观点而言，标准个人电脑 OS 应提供以下功能：进程管理（processing management）、记忆空间管理（memory management）、文件系统（file system）、网络通信、安全机制（security）、使用者界面、驱动程序。目前在大家平时的学习工作中最常见的操作系统主要有 Windows、Linux、UNIX、Mac OS 等。如图 5-1 所示为四种操作系统的不同界面。

2. 数据库系统

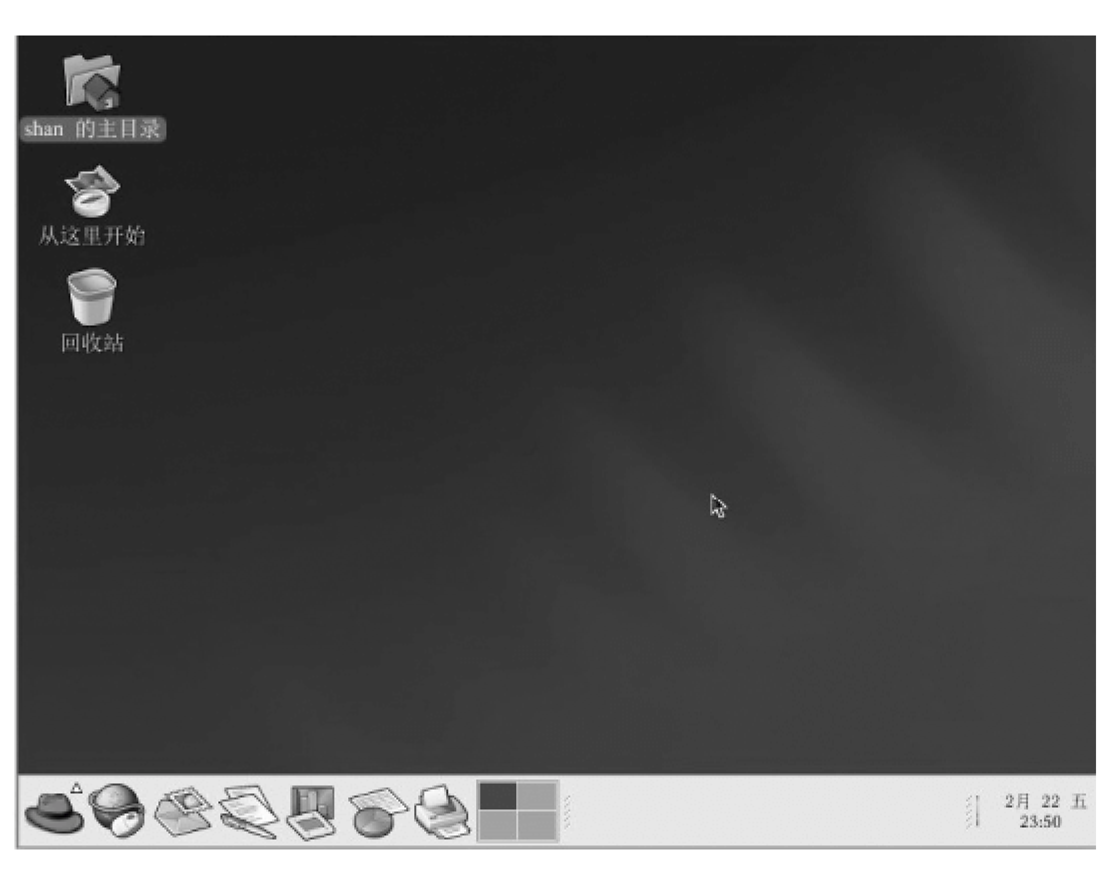
另一种常见的系统软件是数据库系统（database system，DBS）。数据库系统是由数据库及其管理软件组成的系统。它是为适应数据处理的需要而发展起来的一种较为理想的数据处理的核心机构。它是一个实际可运行的存储、维护和为应用系统提供数据的软件系统，是存储介质、处理对象和管理系统的集合体。

数据库系统通常由软件、数据库和数据管理员组成。其软件主要包括操作系统、各种宿主语言、实用程序以及数据库系统。数据库由数据库系统统一管理，数据的插入、修改和检索均要通过数据库系统进行。数据管理员负责创建、监控和维护整个数据库，使数据能被任何有权使用的人有效使用。数据库管理员一般是由业务水平较高、资历较深的人员担任。

具有代表性的数据管理系统有：Oracle、Microsoft SQL Server、Access、MySQL 及 PostgreSQL 等。通常数据库管理员会使用数据库系统来创建数据库系统。



(a) Windows操作系统界面



(b) UNIX操作系统界面



(c) Linux操作系统界面



(d) Mac OS操作系统界面

图 5-1　四种操作系统的不同界面

5.1.2　系统软件安全威胁

1. 操作系统安全威胁

操作系统的安全是整个计算机系统安全的基础，没有操作系统安全，就不可能真正解决数据库安全、网络安全和其他应用软件的安全问题。操作系统面临的安全威胁如下。

（1）恶意代码的破坏和影响。

例如，计算机病毒可以使系统感染，也可以使应用程序或数据文件受到感染，造成程序和数据文件的丢失或破坏，甚至使系统瘫痪或崩溃。

（2）恶意用户的攻击。

人们常常把这些恶意用户称为计算机“黑客”，他们设法获取非授权的资源访问权，危害计算机及其信息系统的保密性和完整性。例如，非法获取其他用户的信息。这些信息可以是系统运行时内存中的信息，也可以是存储在磁盘上的信息（文件）。窃取的方法有多种，可以通过破解其他用户的口令来获取该用户的资源；可以通过执行隐藏在正常程序中的“特洛伊木马”程序秘密窃取，还可以利用隐蔽信道非法访问资源，等等。

(3) 用户的误操作。

用户无意中删除了不想删除的文件,无意中停止了系统的正常处理任务,这样的误操作或不合理地使用了系统提供的命令,会成为对资源的安全威胁。此外,在多用户操作系统中,各用户程序执行过程中相互间会产生不良影响,用户之间会相互干扰。

2. 数据库系统安全威胁

数据是许多企业和组织的核心资产,增强数据库系统的安全性是保护数据的重要环节。对于数据库系统而言,比较突出的安全威胁主要表现在以下几个方面。

(1) 用户权限威胁。

当用户(或应用程序)被授予超出了其工作职能所需的数据库访问权限时,这些权限可能会被恶意滥用。例如,一个大学管理员在工作中只需要能够更改学生的联系信息,不过他可能会利用过高的数据库更新权限来更改分数。

用户还可能将合法的数据库权限用于未经授权的目的。假设一个恶意的医务人员拥有可以通过自定义 Web 应用程序查看单个患者病历的权限。通常情况下,该 Web 应用程序的结构限制用户只能查看单个患者的病史,即无法同时查看多个患者的病历并且不允许复制电子副本。但是,恶意的医务人员可以通过使用其他客户端(如 MS-Excel)连接到数据库,来规避这些限制。通过使用 MS-Excel 以及合法的登录凭据,该医务人员就可以检索和保存所有患者的病历。

这种私自复制患者病历数据库的副本的做法不可能符合任何医疗组织的患者数据保护策略。要考虑两点风险。第一点是恶意的医务人员会将患者病历用于金钱交易;第二点可能更为常见,即员工由于疏忽将检索到的大量信息存储在自己的客户端计算机上,用于合法工作目的。一旦数据存在于终端计算机上,就可能成为特洛伊木马程序以及笔记本电脑盗窃等的攻击目标。

攻击者可以利用数据库平台软件的漏洞将普通用户的权限转换为管理员权限。漏洞可以在存储过程、内置函数、协议实现甚至是 SQL 语句中找到。例如,一个金融机构的软件开发人员可以利用有漏洞的函数来获得数据库管理权限。使用管理权限,恶意的开发人员可以禁用审计机制、开设伪造的账户以及转账等。

(2) 系统平台漏洞。

底层操作系统(Windows 2000、UNIX 等)中的漏洞和安装在数据库服务器上的其他服务中的漏洞可能导致未经授权的访问、数据破坏或拒绝服务。例如,“冲击波病毒”就是利用了 Windows 2000 的漏洞为拒绝服务攻击创造条件。

(3) SQL 注入。

在 SQL 注入攻击中,入侵者通常将未经授权的数据库语句插入(或“注入”)到有漏洞的 SQL 数据信道中。通常情况下,攻击所针对的数据信道包括存储过程和 Web 应用程序输入参数。然后,这些注入的语句被传递到数据库中并在数据库中执行。使用 SQL 注入,攻击者可以不受限制地访问整个数据库。将以下三个技术结合使用可以有效地抵御 SQL 注入:入侵防御系统(Intrusion Prevent System,IPS)、查询级别访问控制和事件相关。IPS 可以识别有漏洞的存储过程或 SQL 注入字符串。但是,单独使用 IPS 并不可

靠，因为 SQL 注入字符串很容易发生误报。如果只依赖 IPS，安全管理人员会发现大量“可能的”SQL 注入警报，被搞得焦头烂额。

(4) 审计记录不足。

自动记录所有敏感的和/或异常的数据库事务应该是所有数据库部署基础的一部分。如果数据库审计策略不足，则组织将在很多级别上面临严重风险。

(5) 身份验证不足。

薄弱的身份验证方案可以使攻击者窃取或以其他方法获得登录凭据，从而获取合法的数据库用户的身份。攻击者可以采取很多策略来获取凭据：

暴力——攻击者不断地输入用户名/密码组合，直到找到可以登录的一组。暴力过程可能是靠猜测，也可能是系统地枚举可能的用户名/密码组合。通常，攻击者会使用自动化程序来加快暴力过程的速度。

社会工程——在这个方案中，攻击者利用人天生容易相信别人的倾向来获取他人的信任，从而获得其登录凭据。例如，攻击者可能在电话中伪装成一名 IT 经理，以“系统维护”为由要求提供登录凭据。

直接窃取凭据——攻击者可能通过抄写即时贴上的内容或复制密码文件来窃取登录凭据。

(6) 备份数据安全威胁。

经常情况下，备份数据库存储介质对于攻击者是毫无防护措施的。因此，在若干起著名的安全破坏活动中，都是数据库备份磁带和硬盘被盗。要防止备份数据暴露，所有数据库备份都应加密。实际上，某些供应商已经建议在未来的数据库管理系统产品中不应支持创建未加密的备份。建议经常对联机的生产数据库信息进行加密。

5.1.3 系统软件安全体系结构

1. 操作系统安全体系结构

操作系统的安全性需要操作系统在基本功能基础上增加安全机制与措施，以保障计算机资源使用的保密性、完整性和可用性。操作系统的安全性处于硬件和上层应用的中间环节，可以对数据库、应用软件、网络系统提供全方位的保护。

操作系统的安全性是其强大功能的有力保证，没有了操作系统的安全性，其功能就好比没有地基的城堡。同时，再安全的操作系统如果不能达到用户对于功能的需求，这样的系统也不会得到应用。

(1) 操作系统安全体系结构内容。

操作系统的安全体系结构主要包含以下几个方面的内容。

① 制定安全服务及措施。

根据系统要达到的安全目标制定要提供的所有安全服务以及保护系统自身安全的所有安全措施。对系统中这些安全相关的所有方面用自然语言或形式语言进行详细描述。

② 构建安全模块之间的关系。

在抽象层次上按满足安全需求的方式来描述系统关键元素即模块之间的关系，描述

方式可以采用逻辑框图。

③ 明确设计的基本原理。

根据系统安全设计的要求以及工程设计的理论和方法来协调设计的各方面安全措施的基本原则。

④ 形成开发过程的大致框架体系与对应的层次结构。

为了正确描述整个开发过程中系统安全需求的各个方面，通常首先进行概念化设计，形成一个大致的安全框架体系，它是安全概念的最高抽象层次的处理，如系统安全策略要求保障程度，系统安全要求对开发过程的影响，以及总体的指导原则。然后，进行功能化设计，在确定系统大致体系的情况下，安全体系必须进一步细化来反映系统的结构。

(2) 操作系统安全体系结构层次和原则。

1993 年，美国国防部推出新的安全体系结构 DGSA (defence goal security architecture)，DGSA 把安全体系根据开发进度划分为四个层次：抽象体系(abstract architecture)、通用体系(generic architecture)、逻辑体系(logical architecture)、具体体系(specific architecture)。

同时，在对操作系统安全体系结构进行设计时需要注意遵循以下几个原则。

① 同步考虑原则。

② 超前设计原则，并且在考虑未来可能面临的安全需求的同时还应注意两个方面：不能把问题定得太特殊或太具体，否则会损失系统的灵活性；不要针对具体问题来理解安全问题，要从适当的抽象层次来完成未来安全需求的足够细化。

③ 机制经济性原则。

④ 限制授权原则。

⑤ 对外开放原则。

⑥ 最小、最少原则。

⑦ 权利分离原则。

⑧ 安全功能结构化设计原则。

⑨ 保持界面友好原则。

(3) 典型安全体系结构。

在安全体系结构方面，目前比较常用和相对成熟的有权能体系结构和 Flask 体系结构。

① 权能体系结构。

通俗地讲，权能就是指主体对客体的访问权力以及能力，权能也可以看成是主体或客体的保护名。目前，人们实现安全比较偏爱的方法之一就是权能体系结构，它是比较早用于实现安全内核的结构体系，具有很强的可塑性与通用性，主要由标识符和域组成。一个好的权能管理模型能够大幅提高基于权能的安全操作系统的性能，包括权能的创建、使用、传播和撤销，其中权能撤销是个难点。目前基于权能的安全操作系统没有很好地解决权能管理问题。

② Flask 体系结构。

Flask(fluke advanced security kernel)是以 Fluke 操作系统为基础开发的安全操作

系统原型。Flask 系统的安全体系结构是从(distributed trusted operating system, DTOS)原型系统的安全体系结构衍生而来的,描述了执行安全策略决策的客体管理器、做决策的安全服务器以及每个子系统组件的需求之间的相互操作,如图 5-2 所示。

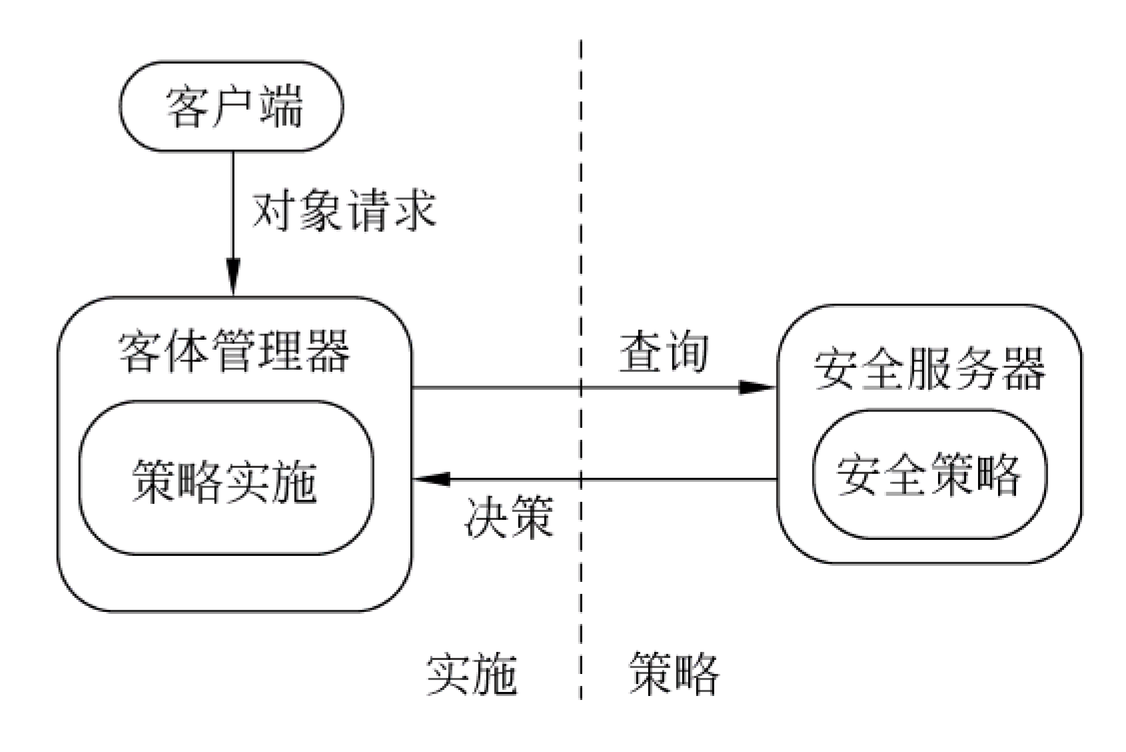


图 5-2 Flask 体系结构组成

DTOS 的安全体系结构是独立于特定安全政策的,但它却存在无法支持动态安全政策的不足。与此相反,Flask 的安全体系结构克服了 DTOS 体系结构中的不足,实现了动态安全政策,支持政策灵活性。Flask 体系包括一个安全策略服务器来制定访问控制决策,一个微内核和系统其他客体管理器框架来执行访问控制决策。

当然研究安全可靠的操作系统,应均衡操作系统功能与安全的关系,不能因注重系统功能而忽视其安全性,也不能因注重系统安全而忽略其功能的重要性。

2. 数据库系统安全体系结构

数据库系统的安全体系结构根据不同级别的数据库而言有所不同,但是从广义上讲,数据库系统的安全框架(data base system security framework)可以划分为以下三个层次。

(1) 网络系统层次。

网络系统是数据库应用的外部环境和基础,网络系统的安全是数据库安全的第一道屏障,外部入侵首先就是从入侵网络系统开始的。

(2) 宿主操作系统层次。

操作系统是大型数据库系统的运行平台,为数据库系统提供一定程度的安全保护。目前操作系统平台大多数集中在 Windows NT 和 UNIX,安全级别通常为 C1、C2 级。主要安全技术有操作系统安全策略、安全管理策略、数据安全等方面。

(3) 数据库系统层次。

数据库系统的安全性很大程度上依赖于数据库系统。如果数据库系统安全机制非常强大,则数据库系统的安全性能较好。

5.1.4 系统软件安全技术

对于不同的系统软件而言,使用的系统软件安全技术也不同。

1. 操作系统安全技术

操作系统的安全防护技术一般可以分为:

(1) 操作系统隔离控制安全技术——隔离、时间隔离控制、逻辑隔离控制和加密隔离控制;

(2) 操作系统访问控制安全技术——自主访问控制、强制访问控制、基于角色的访问控制、域和类型执行的访问控制;

(3) 操作系统资源防护技术，此大类技术又可以从系统登录和用户管理安全、内存管理安全、文件系统安全三方面进行更细化的分类。

2. 数据库系统安全技术

据有关资料报道，80%的计算机犯罪来自系统内部。在传统的数据库系统中，数据库管理员的权利至高无上，既负责各项系统管理工作，例如资源分配、用户授权、系统审计等，又可以查询数据库中的一切信息，为此不少系统以种种手段来削弱系统管理员的权利。实现数据库加密以后，各用户或用户组的数据由用户用自己的密钥加密，数据库管理员获得的信息无法进行正常脱密，从而保证了用户信息的安全。另外，通过加密，数据库的备份内容成为密文，从而能减少因备份介质失窃或丢失而造成的损失。

通用的数据库系统安全技术有用户标识与鉴别、存取控制(自主存取控制方法和强制存取控制方法)、视图审计和数据加密机制。

(1) 用户标识与鉴别。

通过用户标识与鉴别技术来保护数据库系统的主要方法是，首先用输入用户名(用户标识号)来标明用户身份，系统内部记录着所有合法用户的标识，系统对输入的用户名与合法用户名对照，鉴别此用户是否为合法用户，然后通过回答口令标识用户身份，系统常常要求用户输入口令，只有口令正确才能进入系统。为保密起见，口令由用户自己定义并可以随时变更。为防止口令被人窃取，用户在终端上输入口令时，不把口令的内容显示在屏幕上，而用字符“*”替代其内容。最后通过回答对随机数的运算结果表明用户身份。系统提供一个随机数，用户根据预先约定的计算过程或计算函数进行计算，并将计算结果输入计算机，系统根据用户计算结果判定用户是否合法。

(2) 存取控制。

存取控制由两部分构成：

① 定义用户权限，并将用户权限登记到数据字典中。

② 当用户提出操作请求时，系统进行权限检查，拒绝用户的非法操作。

存取控制可分成两种不同的类型：

① 自主存取控制(discretionary access control，DAC)。用户对于不同的对象有不同的存取权限；不同的用户对同一对象的存取权限也各不相同；用户可将自己拥有的存取权限转授给其他用户。

② 强制存取控制(mandatory access control，MAC)。每一个数据对象被标以一定的密级；每一个用户也被授予某一个级别的许可证；对于任意一个对象，只有具有合法许可证的用户才可以存取。

(3) 视图审计和数据加密机制。

为不同的用户定义不同的视图，通过视图把数据对象限制在一定范围内，把要保密的数据对无权存取的用户隐藏起来，从而自动地对数据提供一定程度的安全保护。

审计功能就是把用户对数据库的所有操作自动记录下来放入审计日志中，一旦发生数据被非法存取，DBA 可以利用审计跟踪的信息，重现导致数据库现有状况的一系列事件，找出非法存取数据的人、时间和内容等。

数据加密机制参见第 3 章内容。

5.2　操作系统安全

信息安全问题的核心是信息系统的完整性、可用性和保密性，而在整个信息系统中操作系统是最核心的基础软件，操作系统是计算机中提供安全保护的一个基础设施。操作系统支持应用程序的执行，所以每一层上的安全限制都应在操作系统中得到加强。大多数的安全问题会在计算机主机中体现，因此操作系统的安全问题就是整个计算机安全的基础。

本节主要介绍操作系统的安全机制、安全模型、Windows 操作系统安全与 Linux 操作系统安全。

5.2.1　操作系统安全机制

大多数操作系统都含有某种程度的信息安全机制。信息安全机制主要基于以下两大理念。

(1) 操作系统提供外界直接或间接存取数据资源的管道，例如本地端磁盘机的文件、受保护的特权系统调用（system call）、使用者的隐私数据与系统执行的程序所提供的服务。

(2) 操作系统有能力认证（authorization）资源存取的请求。允许通过认证的请求并拒绝无法通过的非法请求，并将适当的权力授权（authentication）给此请求。有些系统的认证机制仅简略地把资源分为特权或非特权，且每个请求都有独特的身份辨识号码，例如使用者名称。资源请求通常分成两大种类。

第一类（内部来源）通常是一个正在执行的程序发出的资源请求。在某些系统上，一个程序一旦可执行就可做任何事情（例如 DOS 操作时代的病毒），但通常操作系统会给程序一个识别代号，并且在此程序发出请求时，检查其代号与所需资源的存取权限关系。

第二类（外部来源）是从非本地端计算机而来的资源请求，例如远程登入本机计算机或某些网络连接请求（FTP 或 HTTP）。为了识别这些外部请求，系统也许会对此请求提出认证要求。通常是请求输入使用者名称以及相对应的密码。系统有时也会应用诸如磁卡或生物识别数据的其他认证方法。在某些例子，例如网络通信上，通常不需通过认证即可存取资源（例如匿名存取的 FTP 服务器或 P2P 服务）。

除了允许/拒绝形式的安全机制，一个高安全等级的系统也会提供记录选项，允许记录各种请求对资源存取的行为（例如“谁曾经读了这个文件?”）。由于军方与商业组织将敏感数据记录在计算机上，安全机制在操作系统历史上是一个被长久关注与讨论的问题。美国国防部（DOD）便创立了《可信赖之计算机系统评鉴程序》（trusted computer system evaluation criteria，TCSEC），此手册确立了评鉴安全机制成效的基本原则。这对操作系统作者来说非常重要，因为 TCSEC 是用于评鉴、分类与选拔出用于处理、储存与获取敏感或机密数据的计算机系统的标准程序。

1. 内部信息安全

内部信息安全可视为防止正在执行的程序任意存取系统资源的手段。大多操作系统让普通程序可直接操作计算机的 CPU，所以产生了一些问题，例如怎样如操作系统一样处理事务、将执行特殊指令的程序强迫停止。通常权限层级较低的程序想要执行某些特殊指令时会被阻断，例如直接存取硬盘之类的外部设备，程序必须询问操作系统，让操作系统执行特殊指令来存取磁盘。因此操作系统就有机会检查此程序的身份，并依此接受或拒绝它的请求。在不支持特殊指令的硬件上，另一个保护方法，是操作系统不直接利用 CPU 执行使用者的程序，而是模拟一个 CPU 或提供一个 P-Code 系统（伪代码执行机），像 Java 一样让程序在虚拟机上执行。

内部安全机制在多使用者计算机上特别重要：它允许每个系统使用者拥有自己个人的文件与目录，且其他使用者不能任意存取或删除。因为任何程序都可能绕过操作系统的监控，更有可能绕过侧录程序的监控，拥有强制力的内部安全机制在侧录启动时也非常重要。

2. 外部信息安全

通常一个操作系统会为其他网络上的计算机或使用者提供（主持）各种服务。这些服务通常借由端口或操作系统网络地址后的数字存取点提供。通常此服务包括提供文件共享（NTFS）、打印共享、电子邮件、网页服务与文件传输协议（FTP）。外部信息安全的最前线，是诸如防火墙等的硬件设备。在操作系统内部也常设置许多种类的软件防火墙。软件防火墙可设置接受或拒绝在操作系统上执行的服务与外界的连接。因此任何人都可以安装并执行某些不安全的网络服务，例如 Telnet 或 FTP，并且设置除了某些自用通道之外阻挡其他所有连接，以达成防堵不良连接的机制。

5.2.2 操作系统安全模型

1. 安全模型的概念与特征

安全模型描述了对某个安全策略需要用哪种机制来满足；模型的实现则描述了如何把特定的机制应用于系统中，从而实现某一特定安全策略所需的安全保护。孤立的信息是没有价值的，信息只有在需要被识别，被传递及被访问才能产生价值，所以信息的安全，实际上访问控制的安全，即哪些信息可以被哪些群体访问，哪些信息被访问时完整性没有被破坏的，哪些信息是保密的不可以被随便访问。

安全模型精确的描述系统的安全需求和安全策略。具有几个特点：精确、无二义性；简单、抽象、容易理解；具有一般性，仅涉及安全性质不涉及具体的设计和实现。

2. 安全模型的分类

操作系统安全的核心是访问控制，主体对客体的访问只能是授权的，未授权的访问是不能进行的，而且授权策略是安全的。访问控制模型可以分为三大类，一类是自主访问控

制模型 DAC(discretionary access control),客体的属主可以自主地将权限转授给其他主体的模型。第二类是强制访问控制模型 MAC(mandatory access control),即使是客体的属主,也不能自主地将权限转授给其他主体的模型。一个主体能否获得对某客体的权限,要根据安全规则来确定。第三类则是基于角色的访问控制模型。

(1) 自主访问控制模型。

自主访问控制模型(DAC model)是根据自主访问控制策略建立的一种模型,允许合法用户以用户或用户组的身份访问策略规定的客体,同时阻止非授权用户访问客体,某些用户还可以自主地把自己所拥有的客体的访问权限授予其他用户。自主访问控制的实现方式通常包括目录式访问控制模式、访问控制表、访问控制矩阵和面向过程的访问控制等方式。

访问控制表(access control list,ACL)是存在计算机中的一张表,用户对特定系统对象例如文件目录或单个文件的存取控制。每个对象拥有一个在访问控制表中定义的安全属性。这张表对于每个系统用户都拥有一个访问权限。最一般的访问权限包括读文件、写一个或多个文件和执行一个文件。

ACL 是 DAC 中通常采用的一种机制。ACL 是带有访问权限的矩阵,这些访问权是授予主体访问某一客体的。安全管理员通过维护 ACL 控制用户访问企业数据。对每个受保护的资源,ACL 对应一个个人用户列表或由个人用户构成的组列表,表中规定了相应的访问模式。DAC 的主要特征体现在主体可以自主地把自己所拥有客体的访问权限授予其他主体或者从其他主体收回所授予的权限,访问通常基于访问控制表。

为实现完备的自主访问控制,由访问控制矩阵提供的信息必须以某种形式保存在系统中,访问控制矩阵中的每行表示一个主体,每列则表示一个受保护的客体。矩阵中的元素表示主体可对客体的访问模式。目前在操作系统中实现的自主访问控制都不是将矩阵整个保存起来,因为那样做效率很低。实际的方法是基于矩阵的行或列来表达访问控制信息。

① 基于行的自主访问控制方法。

基于行的访问控制方法是在每个主体上都附加一个该主体可访问的客体的明细表。按照表内信息的不同,可以分为三种形式:权利表,该表可确定用户是否可以对客体进行访问,以及可以进行何种访问;前缀表,包括受保护的客体名和主体对它的访问权;口令,口令机制是按行表示访问控制矩阵的,每个客体都相应地有一个口令,主体在对客体进行访问前,必须向操作系统提供该客体的口令。

② 基于列的自主访问控制方法。

基于列的访问控制方法是在每个客体上都附加一份可访问它的主体的明细表。有两种形式。

保护位:保护位机制不能完备地表达访问控制矩阵,但它对所有主体、主体组以及该客体的拥有者指明了一个访问模式集合,拥有者是唯一能够改变客体保护位的主体;

访问控制表:每个客体都有一张访问控制表(ACL),记录该客体可被哪些主体访问以及访问的形式。主体访问控制表可以决定任何一个特定的主体是否可对某一客体进行

访问，它是利用在客体上附加一个主体明细表的方法来表示访问控制矩阵的，表中的每一项包括主体的身份和对该客体的访问权。

(2) 强制访问控制模型(MAC model)。

和自主访问控制模型(DAC model)不同的是，强制访问控制模型(MAC model)是一种多级访问控制策略，它的主要特点是系统对访问主体和受控对象实行强制访问控制，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。

由于 MAC 通过分级的安全标签实现了信息的单向流通，其中最著名的是 Bell-LaPadula 模型和 Biba 模型：Bell-LaPadula 模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露；Biba 模型则具有不允许向下读、向上写的特点，可以有效地保护数据的完整性。

(3) 基于角色的访问控制模型(RBAC model)。

基于角色的访问控制(role-based access control，RBAC)的基本思想就是根据安全策略划分出不同的角色，资源访问许可被封装在角色中，用户被指派到角色，用户通过角色间接地访问资源。

基于角色的访问控制的核心思想就是将访问权限与角色相联系，通过给用户分配合适的角色让用户与访问权限相联系。角色是根据企业内完成各种不同的任务需要而设置的，根据用户在企业中的职权和责任来设定他们的角色。用户可以在角色间进行转换，系统可以添加、删除角色，还可以对角色的权限进行添加、删除。这样通过应用 RBAC，将安全性放在一个接近组织结构的自然层面上进行管理。

RBAC 模型的最大优点在于它能够灵活表达和实现组织的安全政策，使管理员从访问控制底层的具体实现机制中脱离出来，十分接近日常的组织管理规则。RBAC 模型被认为是一种更普遍适用的访问控制模型，可以有效表达和巩固特定事务的安全策略，有效缓解传统安全管理处理瓶颈问题。

总地来说安全模型对于安全计算机系统的设计具有指导意义，并且具有抽象、精确、无歧义等优点，但是安全模型不是技术设计书，不是具体的实现方案。

5.2.3 Windows 操作系统安全

1. 账号安全管理

所谓用户账号，是计算机使用者的身份标识。每一个使用计算机的人，必须凭借个人用户账号才能进入计算机，进而使用计算机中的资源。

用户账号管理不当是导致入侵系统的主要手段。管理员如果能谨慎小心细致地管理账号，可以避免很多潜在的问题，如选择强固的密码、有效的策略加强通知用户的习惯，分配适当的权限等。

在 Windows 操作系统默认设置中 Administrator 是系统管理员账号，具有最高权限。在域中和计算机中具有不受限制的权利，可以管理本地或域中的任何计算机，如创建账

号、创建组、实施安全策略等，系统管理员账号从不被锁定，不能删除但是可重命名。其他账号可由系统管理员账号创建，一般来说由系统管理员账号所创建的账号可被禁用或者删除。

拥有用户账号后，为了提高账号的安全性，可以在操作系统中对账号设置密码，在一定程度上防止操作系统被入侵。

2. Windows 注册表

注册表是 Windows 的数据库，这个数据库存储了计算机软硬件的各种配置数据，相当于中枢神经对于人体而言。因此优化注册表可以把计算机调整到最佳的状态。而黑客对于 Windows 操作系统的入侵手段多数都是借助或篡改注册表而进行的。

PC 机及其操作系统的一个特点就是允许用户按照自己的要求对计算机系统的硬件和软件进行各种各样的配置。早期的 Windows 操作系统，如 Win3. x 中，对软硬件工作环境的配置是通过对扩展名为. ini 的文件进行修改来完成的，但 INI 文件管理起来很不方便，因为每种设备或应用程序都得有自己的 INI 文件，并且在网络上难以实现远程访问。

为了克服上述这些问题，在 Windows 95 及其后继版本中，采用了一种叫做“注册表”的数据库来统一进行管理，将各种信息资源集中起来并存储各种配置信息。按照这一原则，Windows 各版本中都采用了将应用程序和计算机系统全部配置信息容纳在一起的注册表，用来管理应用程序和文件的关联、硬件设备说明、状态属性以及各种状态信息和数据等。

注册表与 INI 文件不同的是：

(1) 注册表采用了二进制形式登录数据；

(2) 注册表支持子关键字，各级子关键字都有自己的“键值”；

(3) 注册表中的键值项可以包含可执行代码，而不是简单的字串；

(4) 在同一台计算机上，注册表可以存储多个用户的特性。

注册表的特点有：

(1) 注册表允许对硬件、系统参数、应用程序和设备驱动程序进行跟踪配置，这使得修改某些设置后不用重新启动成为可能。

(2) 注册表中登录的硬件部分数据可以支持高版本 Windows 的即插即用特性。当 Windows 检测到计算机上的新设备时，就把有关数据保存到注册表中，另外，还可以避免新设备与原有设备之间的资源冲突。

(3) 管理人员和用户通过注册表可以在网络上检查系统的配置和设置，使得远程管理得以实现。

在 Windows 操作系统中通过程序附件进入“命令提示符”窗口，如图 5-3 所示。

在窗口中输入命令“regedit”如图 5-4 所示，可以打开“注册表编辑器”窗口编辑注册表。

注册表包含 5 个主关键字：

(1) HKEY_CLASSES_ROOT：基层类别键，定义了系统中所有已经注册的文件扩

命令提示符
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\lenovo>

图 5-3 “命令提示符”窗口



图 5-4 打开注册表命令语句

展名、文件类型、文件图标等。

(2) HKEY_CURRENT_USER：定义了当前用户的所有权限，实际上就是 HKEY_USERS.Default 下面的一部分内容，包含了当前用户的登录信息。

(3) HKEY_LOCAL_MACHINE：定义了本地计算机(相对网络环境而言)的软硬件的全部信息。当系统的配置和设置发生变化时，其下面的登录项也会随之改变。

(4) HKEY_USERS：定义了所有的用户信息，其中部分分支将映射到 HKEY_CURRENT_USER 关键字中，它的大部分设置都可以通过控制面板来修改。

(5) HKEY_CURRENT_CONFIG：定义了计算机的当前配置情况，如显示器、打印机等可选外部设备及其设置信息等。它实际上也是指向 HKEY_LOCAL_MACHINEConfig 结构中的某个分支的指针。

黑客利用注册表主要包括突破部分网管软件限制、共享特定硬盘分区并运行指定程序、启动黑客程序三方面。表 5-1 列出一些常见的注册表操作，可以方便在使用 Windows 操作系统中提高注册表安全性。

3. Windows 组策略

所谓组，是一组相关账号的集合。可以按照不同用户的操作需求和资源访问需求来创建不同的组，实现对用户的统一配置和管理。使用组的目的是为了简化对网络的管理，通过组可以一次性地为一批用户授权。组是强有力的管理工具之一，使用组可以减少需要直接管理的对象数量，从而简化了网络维护与管理。

在 Windows 操作系统中常用的内置组如下。

表 5-1　常见注册表操作

作　　用	方　　法
禁止显示 IE 的地址栏	HKEY_CLASSES_ROOT\CLSID\\InProcServer32 下在“注册表编辑器”窗口右边中修改字符串“默认”的值为“rem C:\WINDOWS\SYSTEM\BROWSEUI.DLL”
禁止 IE“Internet 选项”中高级项	HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet\Explorer\Control Panel 在“注册表编辑器”窗口右边中新建一个 DWORD 值“AdvancedTab”，并设值为“1”
局域网自动断开的时间	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 在“注册表编辑器”窗口右边新建一个 DWORD 值“Autodisconnect”，并设值为想要设置的分钟数
为同一部计算机设置 2 个 IP 地址	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans 点击 0000、0001，0002…留意“注册表编辑器”窗口右边，当发现右边的字符串“DriverDesc”的值为“TCP/IP”，修改同一窗口中的字符串“IPAddress”和“IPMask”，把 IPAddress 设为 IP 地址，如“198.0.1.9，198.0.1.7”，把“IPMask”设为对应的掩码，如“255.255.255.0，255.255.255.0”
隐藏上机用户登录的名字	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon 在“注册表编辑器”窗口右边新建字符串“DontDisplayLastUserName”，设值为“1”
禁止查找用户	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\FindExtensions\Static\WabFind，删除主键“WabFind”
篡改浏览器默认页	HKEY_LOCAL_MACHINE\software\microsoft\internet explorer\main\default_page_url“default_page_url”这个子键的键值即起始页的默认页

(1) Administrators，管理员组。默认情况下，Administrators 中的用户对计算机/域有不受限制的完全访问权。分配给该组的默认权限允许对整个系统进行完全控制。所以，只有受信任的人员才可成为该组的成员。

(2) Power Users，高级用户组。Power Users 可以执行除了为 Administrators 组保留的任务外的其他任何操作系统任务。分配给 Power Users 组的默认权限允许 Power Users 组的成员修改整个计算机的设置。但 Power Users 不具有将自己添加到 Administrators 组的权限。在权限设置中，这个组的权限是仅次于 Administrators 的。

(3) Users，普通用户组。分配给该组的默认权限不允许成员修改操作系统的设置或用户资料。Users 组提供了一个最安全的程序运行环境。在经过 NTFS 格式化的卷上，默认安全设置旨在禁止该组的成员危及操作系统和已安装程序的完整性。用户不能修改系统注册表设置、操作系统文件或程序文件。Users 可以关闭工作站，但不能关闭服务器。Users 可以创建本地组，但只能修改自己创建的本地组。

(4) Guests，来宾组。按默认值，来宾跟普通 Users 的成员有同等访问权，但来宾账号的限制更多。

(5) Everyone，所有的用户。这个计算机上的所有用户都属于这个组。

4. Windows 文件系统安全

在 Windows 操作系统中 NTFS(new technology file system)文件系统是推荐的文件

系统，因为此文件系统在可靠性和安全性方面具有优势，还因为NTFS文件系统是大容量驱动器必需的。

NTFS可以支持的分区大小可以达到2TB(2048GB)。

相比较其他文件系统而言，NTFS有以下优势。

(1) 权限，可对单个文件设置而不仅仅是对文件夹设置。

(2) 文件加密，大大增强了安全性。

(3) 活动目录，可用来方便地查看和控制网络资源。

(4) 域，它是活动目录的一部分，可用于在简化管理任务的同时微调安全选项。

(5) 磁盘活动故障恢复日志，在发生断电或其他系统问题时，可快速地还原信息。NTFS可以自动地修复磁盘错误而不会显示出错信息。

(6) 硬盘配额，可用于监视和控制单个用户使用的磁盘空间大小。

因为操作系统目录的权限是非常严格的，把Windows操作系统的系统文件放置自己单独的分区内是个明智的选择。对于一般使用计算机的用户来说，一般可将文件系统分为3个区：系统、程序和数据。

尽管这种分区需要额外地策划，但这种做法还是较为科学的，特别是简化了对于目录权限的管理。目录可以根据需要分开，这种策略的结果就是易于管理文件和目录的权限。

5. Windows安全审计

审计是对信息系统访问控制的必要补充，它会对用户使用何种信息资源、使用的时间，以及如何使用(执行何种操作)进行记录与监控。审计和监控是实现系统安全的最后一道防线，它能够再现原有的进程和问题，这对于责任追查和数据恢复是非常必要的。

安全审计提供的功能服务于直接和间接两个方面的安全目标：直接目标包括跟踪和监测系统中的异常事件，间接目标是监视系统中其他安全机制的运行情况和可信度。

所有审计的前提是有一个支配审计过程的规则集。规则的确切形式和内容随审计过程具体内容的改变而改变。在商业与管理审计中，规则集包括对确保商业目标的实现有重要意义的管理控制、过程和惯例。这些商业目标包括资源的合理使用、利率最大化、费用最小化、符合相应的法律法规和适当的风险控制。在计算机安全审计的特殊情况下，规则集通常以安全策略的形式明确表述。

安全审计是通过对所关心的事件进行记录和分析来实现的，因此审计系统包括审计发生器、日志记录器、日志分析器和报告机制等几部分。

(1) 日志的内容。

在理想的情况下，日志应该记录每一个可能的事件，以便分析发生的所有事件，并恢复任何时刻进行的历史情况。然而，这样做显然是不现实的，因为要记录每一个数据包、每一条命令和每一次存取操作，需要的存储量将远远大于业务系统，并且将严重影响系统的性能。因此，日志的内容应该是有选择的。

一般情况下，日志记录的内容应满足以下原则：每个必要的事件，以检测已知的攻击模式；关于系统连续可靠工作的记录。通常，一个事件的日志应包括事件发生的日期和时间、引发事件的用户(地址)、事件源和目的地位置、事件类型、事件成败等。

（2）安全审计的记录机制。

日志的记录可以由操作系统完成，也可以由应用系统或其他专用记录系统完成，大部分情况下都可通过系统调用 Syslog 来记录日志，也可以用 SNMP 记录。

（3）安全审计分析。

通过对日志进行分析，从中发现相关事件信息及其规律是安全审计的根本目的。其主要内容包括：

① 潜在侵害分析，日志分析应能用一些规则去监控审计事件，并根据规则发现潜在的入侵。这种规则可以是由已定义的可审计事件的子集所指示的潜在安全攻击的积累或组合，或者其他规则。

② 基于异常检测的轮廓，日志分析应确定用户正常行为的轮廓，当日志中的事件违反正常访问行为的轮廓，或超出正常轮廓一定的门限时，能指出将要发生的威胁。

③ 简单攻击探测，日志分析应对重大威胁事件的特征有明确描述，当这些攻击现象出现时，能及时指出。

④ 复杂攻击探测，要求高的日志分析系统还应能检测到多步入侵序列，当攻击序列出现时，能预测其发生的步骤。

（4）审计事件查阅。

由于审计系统是追踪、恢复的直接依据，甚至是司法依据，因此其自身的安全性十分重要。审计系统的安全主要是查阅和存储的安全。审计事件的查阅应受到严格的限制，不能篡改日志。

（5）审计事件存储。

审计事件的存储也有安全要求，具体有如下几种：受保护的审计踪迹存储、审计数据的可用性保证和防止审计数据丢失。

5.2.4 Linux 操作系统安全

Linux 系统的安全性已经得到了国际高标准的行业认可，如 Red Hat Enterprise Linux 5 已经通过了国际最高的商业系统安全认证 EAL4＋，并完全符合当中最关键的 CAPP、RBACPP 和 LSPP 这三大安全标准。但这些都只意味着 Linux 操作系统在安全功能上达到了行业的要求，企业若要建立真正安全的系统环境，则还需要系统管理员技术及操作人员安全意识的同步提高，以及完善的系统安全管理规章制度。

Linux 操作系统安全包括多个要素，例如，普通用户的系统安全、超级用户的系统安全、文件系统的安全、进程安全以及网络安全等。只有以上各个要素协调配合才能真正地保证系统不易受到致命的打击。

1. Linux 用户安全管理

Linux 系统管理员的职责之一是保证用户资料安全。其中一部分工作是由用户的管理部门来完成的。但作为系统管理员，有责任发现和报告系统的安全问题。

系统管理员可以定期随机抽选一用户，将该用户的安全检查结果发送给他及其管理部门。此外，用户的管理部门应该强化安全意识，制订完善的安全管理规划。

超级用户在安全管理方面需要注意如下事项：

(1) 在一般情况下最好不使用 root 账号，应使用 su 命令进入普通用户账号。

(2) 超级用户不要运行其他用户的程序。

(3) 经常改变 root 口令。

(4) 精心地设置口令时效。

(5) 不要未退出系统就离开终端。

(6) 建议将登录名 root 改成其他名称。

(7) 注意检查不寻常的系统使用情况。

(8) 保持系统文件安全的完整性。

(9) 将磁盘的备份存放在安全的地方。

(10) 确保所有登录账号都有用户口令。

(11) 启动记账系统。

2. 文件系统权限管理

在 Linux 系统中，文件还具有特殊的意义，因为在 Linux 系统中一切都当作文件来看待，如目录、设备、管道等。把对设备的操作实现为对文件的操作。Linux 系统不必再实现一套操作设备的指令，只需要利用现有的对文件操作的指令即可，这样可降低系统的复杂性，提高系统的可靠性并方便用户使用。

所谓的文件权限，是指对文件的访问权限，包括对文件的读(r)、写(w)、执行(x)。对应的权限分别为 4、2、1。Linux 文件系统的安全主要通过设置文件的权限来实现。每一个 Linux 的文件或目录，都有 3 组属性，分别表示文件的所有者、文件所属组用户、系统中的其他用户(只读、可写、可执行、允许 SUID、允许 SGID 等)。特别注意，权限为 SUID 和 SGID 的可执行文件，在程序运行过程中，会给进程赋予所有者的权限，如果被黑客发现并利用就会给系统造成危害。通常，对于系统中的一些关键文件，如/etc、/bin、/boot、/dev 等目录下的文件，将它们设置为只读将大大提高文件系统的安全性。例如，将 passwd 文件属性修改为只有文件的拥有者 root 可以读写该文件，可以使用命令 chmod 600/etc/profile 或 chmod u+rw/etc/profile，这样可保证只有超级用户才可以读写该文件，加强 Linux 系统的安全管理。除此之外，root 账户可以为 Linux 系统中的所有用户设置默认的访问权限，减少因默认权限设置不当引起的问题。使用 umask 命令可以设置新的文件权限。Linux 默认 umask 值是 022，这样创建的文件属性就是 755，可以防止其他用户修改该用户的文件。由于每个用户都拥有并属于自己的一个私有组，因此不需要在组权限上设置多做考虑。建议 umask 的值设置为 0077，只保证所有者自己的读写即可，在有其他使用情况时，可以将权限适当地由小到大逐渐放开。

3. 日志安全管理

Linux 系统中的日志子系统对于系统安全来说非常重要，它记录了系统每天发生的各种各样的事情，包括哪些用户曾经或者正在使用系统，可以通过日志来检查

错误发生的原因,更重要的是在系统受到黑客攻击后,日志可以记录下攻击者留下的痕迹,通过查看这些痕迹,系统管理员可以发现黑客攻击的某些手段以及特点,从而能够进行处理工作,为抵御下一次攻击做好准备。

在 Linux 系统中,有三类主要的日志子系统。

(1) 连接时间日志:由多个程序执行,把记录写入到/var/log/wtmp 和/var/run/utmp,login 等程序会更新 wtmp 和 utmp 文件,使系统管理员能够跟踪谁在何时登录到系统。

(2) 进程统计:由系统内核执行,当一个进程终止时,为每个进程往进程统计文件(pacct 或 acct)中写一个记录。进程统计的目的是为系统中的基本服务提供命令使用统计。

(3) 错误日志:由 syslogd(8)守护程序执行,各种系统守护进程、用户程序和内核通过 syslogd(3)守护程序向文件/var/log/message 报告值得注意的事件。

4. 网络安全管理

Linux 属于开放性的操作系统,当一台计算机连入网络时,计算机就会存在网络安全问题,因为计算机在通过网络为用户提供正常的网络服务的同时,也存在被非法使用和破坏的危险,但是,提供网络服务是必要的,不能因为网络存在危险而停止服务,因此,必须通过增强网络安全性的各种设置来提高计算机抵御危险的能力。在 Linux 网络安全中防火墙在保证 Linux 网络安全中起了重要作用。

所谓防火墙就是在可以信任的本地网络和不可信任的外部网络之间的一个阻塞点,内部网络和外部网络之间所有的数据流量都必须通过这一个阻塞点。其作用和详细介绍在本书其他章节会有介绍,此处就不再赘述。在 Linux 系统中,Iptables 是 Linux 默认的防火墙软件。它不仅功能强大,而且配置也十分灵活。防火墙设置有两个网卡:一个由内往外发送数据,另一个由外往内发送数据。

5. 信息通路保护

信息通路指信息在操作系统中经过的道路。对信息道路的保护涉及两个方面:一方面对显示信息道路的保护,防止非法信息经过显示道路;另一方面,要堵住隐蔽的信息通路,防止恶意用户通过隐蔽信道进出。

正常信道的保护机制是由可信通路(trusted path)提供的。可信通路是终端人员能借以直接同可信计算基(TCB)通信的一种机制,该机制只能由有关终端人员或可信计算基启动,并且不能被不可信软件模仿。可信通路机制主要应用在用户登录或注册时。

可信通路机制一般是以安全注意键(secure attention key,SAK)为基础实现的。SAK 是由终端驱动程序检测到的键的一个特殊组合。每当系统识别到用户在一个终端上输入的 SAK,便终止对应到该终端的所有用户进程,启动可信的会话过程,以保证用户名和口令不被窃走。Linux 系统的可信通路工作流程如图 5-5 所示。

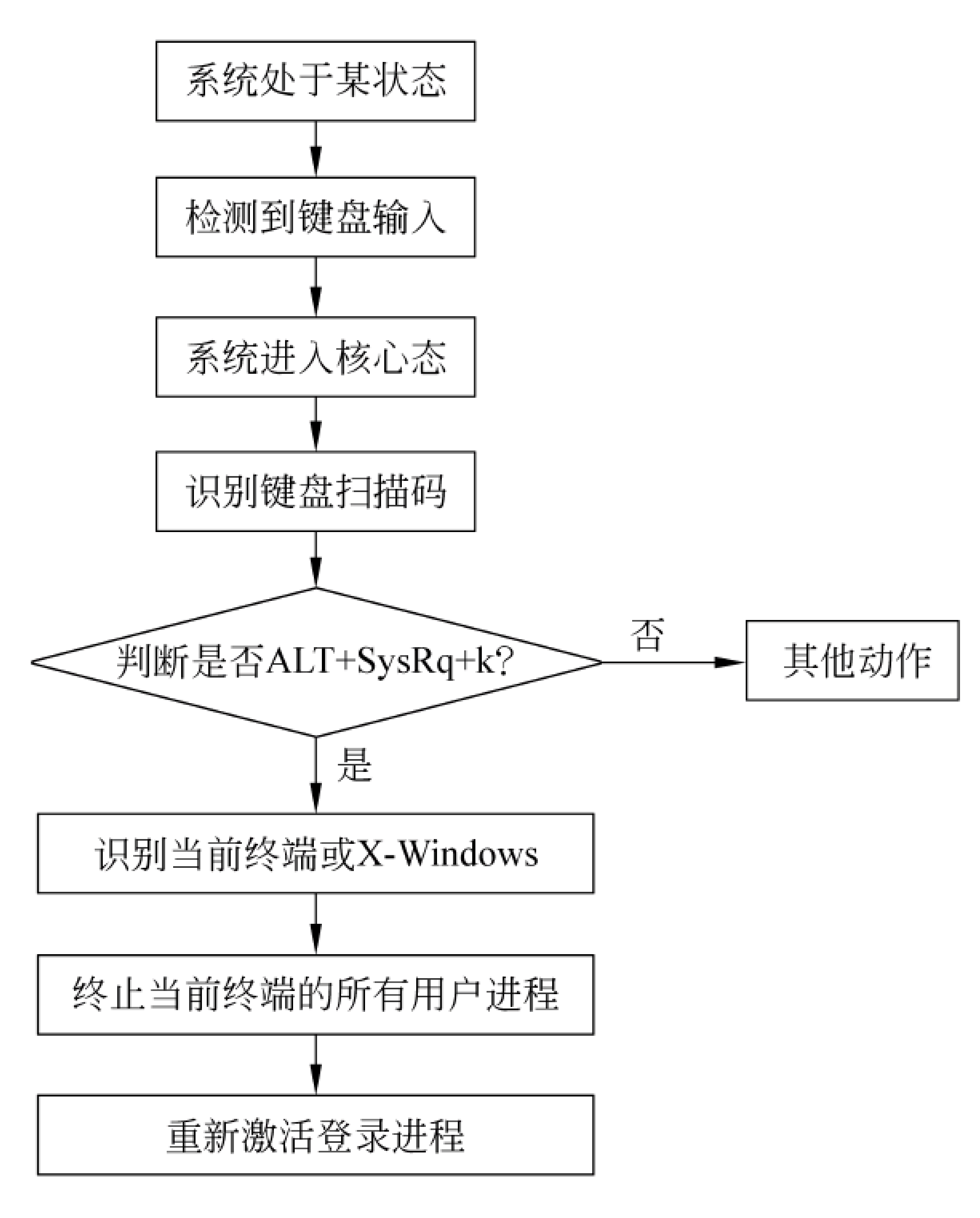


图 5-5　Linux 系统的可信通路工作流程

5.3　数据库系统安全

数据库系统安全是指为数据库建立的安全保护措施,以保护数据库系统软件和其中的数据不因偶然和恶意的原因而遭到破坏、更改和泄露。

本节将通过对不同级别的代表性数据库,对数据库系统的安全需求和数据库系统的安全机制展开阐述。

5.3.1　数据库安全系统特性

1. 数据独立性

数据独立于应用程序之外。理论上数据库系统的数据独立性分为以下两种。

(1) 物理独立性。数据库的物理结构的变化不影响数据库的应用结构,从而也就不能影响其相应的应用程序。这里的物理结构是指数据库的物理位置、物理设备等。

(2) 逻辑独立性。数据库逻辑结构的变化不会影响用户的应用程序,数据类型的修改、增加、改变各表之间的联系都不会导致应用程序的修改。

这两种数据独立性都要靠 DBMS 来实现。到目前为止,物理独立性已经能基本实现,但逻辑独立性实现起来非常困难,数据结构一旦发生变化,一般情况下,相应的应用程序都要作适当的修改。追求这一目标也成为数据库系统结构复杂的一个重要原因。

2. 数据安全性

一个数据库能否实现防止无关人员得到他不应该知道的数据，是数据库是否实用的一个重要指标。如果一个数据库对所有的人都公开数据，那么这个数据库就不是一个可靠的数据库。

一般来说，比较完整的数据库对数据安全性采取以下措施。

(1) 将数据库中需要保护的部分与其他部分相隔离。

(2) 使用授权规则。这是数据库系统经常使用的一个办法，数据库给用户 ID 号和口令、权限。当用户用此 ID 号和口令登录后，就会获得相应的权限。不同的用户或操作会有不同的权限。例如，对于一个表，某人有修改权，而其他人只有查询权。

(3) 将数据加密，以密码的形式存于数据库内。

3. 数据的完整性

数据完整性这一术语用来泛指与损坏和丢失相对的数据状态。它通常表明数据在可靠性和准确性是可信赖的，同时也意味着数据有可能是无效的或者不完整的。数据完整性包括数据的正确性、有效性和一致性。

4. 并发控制

如果数据库应用要实现多用户共享数据，就可能在同一时刻多个用户要存取数据，这种时间叫做并发时间。当一个用户取出数据进行修改，在修改存入数据库之前如有其他用户再取此数据，那么读出的数据就是不正确的。这时就需要对这种并发操作施行控制，排除和避免这种错误的发生，保证数据的正确性。

5. 故障恢复

当数据库运行时出现物理或逻辑上的错误时，如何尽快将它恢复正常，这就是数据库系统的故障恢复功能。

5.3.2 数据库的数据安全保护

数据库中的数据遭到破坏会造成难以估量的损失，所以数据库的数据安全保护是数据库运行过程中一个不可忽视的方面。数据库系统必须建立自己的保护机制，提供数据保护。

安全性问题是所有计算机系统共有的问题，并不是数据库系统特有的，但由于数据库系统数据量庞大且多用户存取，安全性问题就显得尤其突出。由于安全性问题有系统问题与人为问题，所以一方面我们可以从法律、政策、伦理、道德等方面控制约束人们对数据库的安全使用，另一方面还可以从物理设备、操作系统等方面加强保护，保证数据库的安全。另外，可以从数据库本身实现数据库的安全性保护。

在一般的计算机系统中，安全措施是一级一级、层层设置的。

1. 用户标识和鉴定

通过核对用户的名字或身份(ID),决定该用户对系统的使用权。数据库系统不允许一个未经授权的用户对数据库进行操作。

系统让用户用身份和口令登录时,系统用一张用户口令表去鉴别用户身份。表中只有两个字段:用户名和口令,并且用户输入的口令并不显示在屏幕上而是以某种符号代替。系统根据用户的输入鉴别此用户是否为合法用户。这种方法简便易行,但保密性不是很高。

另外一种标识鉴定的方法是用户先标识自己,系统提供相应的口令表,这个口令表不是简单地与用户输入的口令比较,若相等就合法,而是系统给出一个随机数,用户按照某个特定的过程或函数进行计算后给出结果,系统同样按照这个过程或函数对随机数进行计算,如果与用户输入的相等则证明此用户为合法用户,可以再接着为用户分配权限。否则,系统认为此用户根本不是合法用户,拒绝进入数据库系统。

2. 存取控制

对于存取权限的定义称为授权。这些定义经过编译后存储在数据字典中。每当用户发出数据库的操作请求后,数据库管理系统会查找数据字典,根据用户权限进行合法权检查。若用户的操作请求超出了定义的权限,系统拒绝此操作。授权编译程序和合法权检查机制一起组成安全性子系统。

数据库系统中,不同的用户对象有不同的操作权利。对数据库的操作权限一般包括查询权、记录的修改权、索引的建立权、数据库的创建权。把这些权利按一定的规则授予用户,以保证用户的操作在自己的权限范围之内。授权规则可以用表 5-2 表示。

表 5-2　授权规则表

	关系 S	关系 C	关系 SC
用户 1	NONE	SELECT	ALL
用户 2	SELECT	UPDATE	SELECT DELETE UPDATE
用户 3	NONE	NONE	SELECT
用户 4	NONE	INSERT SELECT	NONE
用户 5	ALL	NONE	NONE

数据库的授权由 SQL 的 GRANT(授权)和 REVOKE(回收)来完成。

例如:

将表 TABLE1 的查询权利授予所有用户,语句为:

```
GRANT SELECT ON TABLE TABLE1 TO PUBLIC;
```

将表 TABLE1 的所有权权利授予用户 LI:

```
GRANT ALL PRIVILEGES ON TABLE TABLE1 TO LI;
```

把用户 LI 对 TABLE1 的查询权收回：

```
REVOKE SELECT ON TABLE TABLE1 FROM LI
```

下面是三个安全性公理，将(2)和(3)都假定允许用户更新数据。

(1) 如果用户 I 对属性集 A 的访问(存取)是有条件的选择访问(带谓词 P)，那么用户 I 对 A 的每个子集也是可以有条件的选择访问(但没有一个谓词比 P 强)；

(2) 如果用户 I 对 A 的访问时有条件的更新访问(带谓词 P)，那么用户 I 对 A 也可以是有条件的选择访问(但谓词不能比 P 强)；

(3) 如果用户 I 对属性 A 不能进行选择访问，那么用户 I 也不能对 A 有更新访问。

3. 数据分级

有些数据库系统对安全性的处理是把数据分级。这种方案为每一数据对象(文件、记录或字段等)赋予一定的保密级。例如，绝密级、机密级、秘密级和公用级。对于用户也分成类似的级别。系统便可规定两条规则：

(1) 用户 1 只能查看比他级别低的或同级的数据。

(2) 用户 2 只能修改和他同级的数据。

这个规则要求：用户 2 不能修改比他级别高的数据，同时也不能修改级别比他低的数据，这是为了管理上的方便。如果用户 2 要修改比他级别低的数据，可以修改用户 2 的级别或提高数据的级别使得两者之间的级别相等才能进行修改操作。

数据分级法是一种独立于值的一种简单的控制方式。它的优点是系统能执行“信息流控制”。在授权矩阵方法中，允许凡有权查看秘密数据的用户就可以把这种数据复制到非保密的文件中，那么就有可能使无权用户也可解除秘密数据。在数据分级法中，就可以避免这种非法的信息流动。

然而，这种方案在通用数据库系统中不十分有用，只在某些专用系统中才有用。

4. 数据加密

为了更好地保护数据的安全性，用密码存储口令、数据，对远程终端信息用密码传输防止中途非法截获等。更详细的加密解密介绍在第 3 章有所介绍，此处就不再赘述。

5.3.3 Access 数据库系统安全

Access 是 Microsoft 公司始于 1994 年发表的微机数据库系统。作为一种功能强大的 MIS 系统开发工具，它具有界面友好，易学易用，开发简单，接口灵活等特点，是一个典型的新一代数据管理和信息系统开发工具。与 Microsoft 的其他数据库产品如 FOXPRO 等相比，Access 具有较独特的优势——提供了更强大的数据组织、用户管理、安全检查等功能。在一个工作组级别的网络环境中，使用 Access 开发的多用户数据库系统具有传统的 XBASE 数据库系统所无法比拟的客户服务器(client/server，C/S)结构和相应的数据库安全机制。

1. 建立 Access 的安全系统

(1) 创建 Access 工作组。

一个 Access 工作组定义为一组用户,他们共享一个或多个 Access 应用程序,并且在他们的 Access 副本中附加公共的 SYSTEM. MDA 库。由 Access 的系统管理员(Admin 用户)来给这些用户授予对数据库系统的相应的操作权限,这样,不同的用户就能以不同的权限访问相关的数据库资源。

Access 提供了一个新的应用程序 Microsoft Access Workgroup Administrator,它能自动完成 Access 工作组的创建工作。对一个工作组而言,Access 系统管理员需要用这个程序创建一个新的 SYSTEM. MDA(或用其他任意的文件名 *. MDA)库,并把工作组中的每个用户的 Access 指向这个新的 SYSTEM. MDA。可以这样理解,一个系统数据库 *. MDA 对应一个工作组。

(2) 创建工作组中的 Access 账户。

Access 账户包括 Access 组与 Access 用户。一个 Access 组由一个或多个 Access 用户成员构成。在 Access 的安装过程中,Access 自动默认建立了两个用户组(Admins 与 Users)和一个用户(Admin),这两个用户组与 Admin 用户是不允许删除的。以 Admins 用户组中的用户(如 Admin)登录(LOGIN)进入 Access 后,可以创建新的 Access 组与用户,并将新用户放置到相应的组中。

Admins 组是 Access 的管理员组,默认时只包括 Admin 用户,该组中的用户默认对数据库具有全权,并且可以管理其他的用户和用户组。Users 组是 Access 的默认用户组,每个用户,包括 Admin 及新建用户都属于该组,默认时,Users 组中的用户对数据库也具有全权。

(3) 设置 Admin 用户的登录口令。

Admin 用户的登录口令是整个数据库系统的安全入口,为什么这样说呢?因为如果没有 Admin 登录口令,所有用户的 Access 副本均以 Admin 用户的身份登录数据库,而不是以 Access 管理员所创建的用户名进行登录,只有设置了 Admin 的登录口令,Access 才启动它的安全系统,这也就是为什么无法删除 Admin 用户的原因。

(4) 分配数据库权限。

数据库权限是针对某个具体的数据库而言的。Access 系统管理员(Admins 组中的一个用户)在打开一个需要工作组共享的数据库之后,就可以根据具体情况对工作组中的 Access 组与 Access 用户进行权限的分配了。不同的 Access 数据库对象具有不同的权限集合,Access 的数据库对象包括 6 种,分别是表、查询、表单、报表、宏和模块,必须分别予以授权。对 Access 组的授权适用于该组中的每一个用户。

在这里需要强调指出的是:必须首先屏蔽 Users 组对数据库的所有权限,因为所有 Access 用户都属于 Users 组,而 Users 组默认数据库对象是具有全权的,所以在确定数据库权限之前,必须首先屏蔽掉所有权限。不理解微软为什么要给 Users 组对数据库的全部许可权,在实践中这是一个错误,它毫无意义地增加了 Access 管理员的工作强度与难度(因为经常会有忘记屏蔽 Users 组权限而使整个安全系统形同虚设的事情发生)。所

以，Users 组对数据库对象应默认为具有最低的权限，这样才是最有效和安全的。

2. 消除 Access 的安全漏洞

（1）由 Admin 用户引发的安全漏洞。

因为 Admin 用户是 Access 系统的默认用户，也就是说，除非 Access 系统在安装后已经重新链接到某个新的工作组安全系统上，否则将以默认的 Admin 用户登录 Access。而微软将其用于标记该 Admin 账户的用户 ID 号设成了一个固定值，这就意味着全世界的 Access 系统的 Admin 用户在 Access 中都是同一个用户。这样，问题就出现了——如果一个未链入工作组安全系统的用户在网络文件系统级别上可以获得对此数据库系统文件的 Admin 权，则将以 Admin 用户的身份拥有对该数据库系统的所有权利，由 Access 本身建立起来的第二级安全机制将不起任何作用。这种情况实在太容易发生，工作组用户只要在个人计算机上重新安装一次 Access 软件，便将会轻而易举地避开你设置的安全系统的防护，而作为默认的 Admin 用户登录并操作工作组中任何数据库系统。

（2）解决方案。

解决的基本思路就是屏蔽 Admin 用户对数据库的所有权限，首先，在 Admins 用户组中增加一个新的与 Admin 用户等同的新用户，例如为“www”，然后以这个新用户登录 Access，从 Admins 用户组将 Admin 用户撤出，并屏蔽掉 Admin 用户对数据库的所有权限，这样，Admin 用户就成了一个普通用户，实际的数据库系统管理员则变为新用户“www”，而你的数据库安全系统就对所有的用户起安全防护作用了。

3. 设置数据库密码

最简单也是安全性最低的对 Access 数据库系统的保护方法是对数据库进行加密。加密数据库就是将数据库文件压缩，从而使某些实用程序（如字处理器）不能解读这些文件。加密一个不具有安全设置的数据库并不能保证数据库的安全，因为任何人都可以打开数据库并完全访问数据库中的所有对象。

加密可以避免在以电子方式传输数据库或者将其存储在软盘、磁带或光盘上时，其他用户偶然访问数据库中的信息。然而 Jet（Access 使用的数据库引擎）使用的加密方法非常薄弱，因此绝不能用于保护敏感数据。“加密/解密数据库”命令位于“工具”菜单的“安全”子菜单中。解密数据库是对加密过程的逆运算。

同时可以在数据库上设置密码，从而要求用户在访问数据和数据库对象时输入密码，但是要注意，使用密码保护数据库或其中的对象的安全性也称为共享级安全性。不能使用此选项为用户或组分配权限，因此任何掌握密码的人都可以无限制地访问所有 Access 数据和数据库对象。“设置数据库密码”命令位于“工具”菜单的“安全”子菜单中。

4. 用户级安全机制

除共享级安全性外，还可以使用用户级安全性，它提供了最严格的访问限制，使用户能够最大限度地控制数据库及其中包含的对象。这是在使用 Access 数据库系统中所推荐的数据库保护措施的一部分（当和操作系统提供的文件级和共享级安全性结合使用时）。

用户级安全性(在单独使用时)主要用于保护数据库中的代码和对象,以免用户不小心进行了修改或更改。如果不希望用户非法访问窗体、报表或模块中的代码,则必须将.mdb文件转换为 MDE 文件。要避免用户修改数据库中的查询、宏或数据访问页,唯一的方法就是将数据库文件放在一个受保护的文件共享区域中。此外,在 Access 中不可能既允许用户修改表中的数据,同时又禁止其修改表的设计或删除表。要提供这样一种功能,需要使用一个基于服务器的数据库产品,例如 Microsoft SQL Server。

用户级安全机制不能用于在 Access 2007 中创建的数据库(.accdb 文件)。此外,如果将.mdb 文件转换为新格式(.accdb 文件),那么 Access 2007 会丢弃用户级安全机制设置。Access 2003 和更低版本的 Access 中的用户级安全机制使用密码和权限的组合,即用来指定用户对数据库中数据或对象的访问类型的一组属性。使用时可以为个人或组设置密码和权限,然后这些密码和权限的组合便会成为安全账户,这些账户可以用来定义允许访问数据库中对象的用户和用户组。相应地,用户和组的组合称为工作组,Access 会将该信息存储在工作组信息文件中。当 Access 启动时,它会读取工作组信息文件并根据文件中的数据来确定哪些用户和组具备相应权限。

5. 管理数据库权限

在 Access 2000 中,用户所具有的数据库访问权限有两种类型:显式权限和隐式权限。显式权限是指直接授予某一用户账号的权限,这是该用户账号专用的,与其他用户无关。隐式权限是指授予组账号的权限,即用户加入到组中的同时被赋予的组的权限。如果一个用户同时具有上述两种权限,当该用户对设置了安全性的数据库进行访问时,那么,用户所具有的权限就是两种权限的交集。

在 Access 数据库中,对组和用户访问数据库权限的设置工作,只能通过管理员完成。设置的权限包括打开/运行、读取设计、修改设计、管理、读取数据、更新数据、插入数据和删除数据。

设置和修改用户权限,需要以管理员身份登录,启动数据库。同样需要注意的是,用户权限的设置和更改也只有在 Access 2003 以及更早以前的版本中设置,Access 2003 以后的版本可以保存之前设置的用户权限,但是不能更改。单击“工具/安全/用户与组的权限”,弹出“用户与组的权限”窗口,该窗口中间有“用户”和“组”两个单选按钮,分别用来更改用户或组的权限。组的权限包含了用户的权限,如果组的权限允许更新数据,则用户有权更新数据,不管用户的权限中是否选中该项许可权。在对象类型中选择设置权限的对象,包括表、查询、窗体、报表、宏和模块。在对象名称框内列出了对象的全部内容。例如,如果对象的类型是表,则列出全部表的名称,可以选择一个、多个或全部表。设置权限只要单击窗口下部的复选按钮(检查框)即可,选择完毕后,单击【确定】按钮。通过修改组的权限,一个组的全部用户便具有相同的权限。例如要撤销用户组的修改设计权限,那么属于用户组的用户进入数据库后,就无权修改设计。

5.3.4 SQL Server 数据库系统安全

Microsoft SQL Server 是微软公司推出的企业级网络数据库系统,由于具有良好的

稳定性、可靠性、易操作性及强大的功能，深受用户的青睐，是目前比较流行的商用数据库系统之一。为了实现 SQL Server 数据库的安全性，微软公司建立了既灵活又强大的安全管理机制，它能够对 SQL Server 数据库的安全进行全面管理，安全体系非常具有代表性。

1. 身份验证

对用户的身份认证是数据库系统提供的最外层安全保护措施，其方法是用户进入系统时通过输入 ID 和密码，向系统出示自己的身份证明，系统通过严格的认证机制对用户身份进行审查核实，经过确认后才提供与之相对应的系统服务。SQL Server 支持 Windows NT 认证模式和混合认证模式两种身份认证模式。

(1) Windows NT 认证模式。

在该模式下，使用 Windows NT 操作系统的安全机制验证用户身份。当用户通过 Windows NT 认证并成功登录后，在连接数据库时，SQL Server 直接接收用户的连接请求。

(2) 混合认证模式。

它又称为 SQL Server 认证模式，在这种模式下，用户要用 SQL Server 的登录标识和口令登录，当登录账户和口令通过认证后，用户应用程序才可连接到服务器，否则服务器将会拒绝用户的连接请求。

为了提高 SQL Server 数据库系统的安全性，在任何可能的时候，都应该对指向 SQL Server 的连接要求 Windows 身份验证模式。它通过限制 Microsoft Windows 用户和域用户账号的连接，保护 SQL Server 免受大部分 Internet 工具的侵害，而且，服务器也将从 Windows 安全增强机制中获益，例如更强的身份验证协议以及强制的密码复杂性和过期时间。另外，凭证委派(在多台服务器间桥接凭证的能力)也只能在 Windows 身份验证模式中使用。在客户端，Windows 身份验证模式不再需要存储密码。存储密码是使用标准 SQL Server 登录的应用程序的主要漏洞之一。

2. 审计功能

SQL Server 提供的审计功能是一个十分重要的安全措施，能提供较为完善的审计功能，它用来监视各用户对数据库施加的动作。

审计方式分用户审计和系统审计两种。用户启用审计功能时，SQL Server 的审计系统可记下所有对该数据库表或视图进行访问的企图(包括成功的和不成功的)及每次操作的用户名、时间、操作代码等信息。这些信息一般都被记录在数据字典中，用户可以利用这些信息进行审计分析。系统审计由系统管理员进行，其审计内容主要是系统一级命令以及数据库客体的使用情况。

3. 完整性机制

数据库的完整性机制用于规定数据库中的数据应满足的语义，并对其进行检查，以保证数据的正确性和相容性。SQL Server 提供了完善的数据完整性定义和检查机制，可以通过 SQL 语句或企业管理器中的可视化界面进行完整性定义，不用额外书写代码，可以

有效地支持数据的实体完整性、参照完整性检查，并且提供比较灵活的用户自定义完整性定义检查机制。

(1) 实体完整性在 SQL Server 实际运用中，建表时可以用 PRIMARY KEY 子句定义主码或在企业管理器中指定主码，在用户程序每次对主码进行插入、删除、修改等更新操作时，SQL Server 自动进行完整性检查，若操作违反要求，则拒绝操作和给出错误信息。

(2) 参照完整性在 SQL Server 中，可以通过 FOREIGN KEY 和 REFERENCES 短语或在企业管理器中指定的方式定义主表与从表间的参照关系，当主表删除元组、修改数据或子表插入元组、修改数据时，SQL Server 自动进行完整性检查，若此操作违反要求，则按用户自己选择处理参照关系中对应元组的方法给出处理及相关信息。

(3) 自定义完整性 SQL Server 提供了全面而灵活的自定义完整性定义途径，可分为属性上的约束条件定义和元组上约束条件的定义，前者定义利用如 SQL 语句中的列值非空(NOT NULL)，列值唯一(UNIQUE)，检查列值是否满足一个布尔表达式(CHECK)以及属性的数据类型、企业管理器中的属性取值约束、掩码等方式定义完整性要求；后者的定义则主要利用 CHECK 子句等进行定义，当定义成功，在用户程序进行插入、删除、修改等更新操作时，SQL Server 自动进行自定义完整性检查，若操作违反要求，则给出错误信息。

此外，SQL Server 还提供了触发器机制。当对数据库表进行插入、更新和删除操作时，触发器自动能够根据实际情况触发执行，产生一系列的操作或回退那些破坏数据库完整性的操作。触发器可以包含非常复杂的程序设计逻辑，能提供约束、规则和默认的功能。

4. 服务权限限制

SQL Server 和 SQL Server Agent 是作为 Windows 服务运行的。每个服务必须与一个 Windows 账户相关联，并从这个账户中衍生出安全性上下文。SQL Server 允许 SA (超级管理员)登录的用户(有时也包括其他用户)来访问操作系统特性。这些操作系统调用是由拥有服务器进程的账户的安全性上下文来创建的。如果服务器被攻破，那么这些操作系统调用可能被用来向其他资源进行攻击。因此，限制 SQL Server 的服务权限十分重要。

(1) SQL Server Agent/MSSQL Server。如果拥有指定实例，那么它们应该被命名为 MS SQL Instance Name，作为具有一般用户权限的 Windows 域用户账户运行，不要作为本地系统、本地管理员或域管理员账户运行。

(2) SQL Server Agent Service/SQL Server Agent。如果环境中不需要，则禁用该服务；否则应作为具有一般用户权限的 Windows 域用户账户运行。不要作为本地系统、本地管理员或域管理员账户运行。

5.3.5 Oracle 数据库系统安全

随着计算机网络应用的普及和提高，Oracle 作为大型数据库的代表以其优异的性能

在各个领域得到广泛应用。

1. 系统安全性策略

系统安全策略的定义为：系统安全策略是数据库系统为达到安全目标和相应的安全级别所定义的安全技术、方法、机制的总和。DBMS 将系统安全策略体现在其软件中，最后由 DBA 给予实现，主要体现在安全管理。Oracle 9i 的系统安全策略主要功能如下：

（1）系统与数据的安全性策略。

数据库主要是由数据库用户（DBU）访问的。DBA 可授权 DBU 应用 Create、Alter、Drop 语句对数据库对象的操作权限和用户身份进行验证。数据库用户可以通过操作系统、网络服务、数据库或者安全套接字层 SSL 进行身份确认。

（2）操作系统（OS）安全性。

由于 Oracle 数据库和应用程序是运行在网络操作系统（NOS）之上，然后进行安全认证的，所以前两者的安全性需要与操作系统安全一同考虑。DBA 必须具有对 NOS 的文件进行 Create 和 Delete 的权限而数据库用户却不具有。如果操作系统为数据库用户分配角色，则 DBA 必须有修改操作系统账户安全区域的操作系统权限。

2. 用户安全性策略

在 Oracle 数据库中，将用户分为一般用户、最终用户、数据库管理员（DBA）、应用程序员和应用程序管理员。

由于一般用户和管理员具有相对的普遍性，在此只针对一般用户和管理员的安全性策略进行介绍。

（1）一般用户的安全性策略。

口令安全性。如果是通过数据库进行用户身份验证，就应该使用口令加密方式与数据库进行连接。当执行分布式查询时，会发生在两个 Oracle 服务器之间建立连接。

当试图连接到一个服务器时，Oracle 在将信息发送到服务器时对口令进行加密。如果连接失败且审计可用时，这个失败作为审计日志记录下来。Oracle 就会用加密的信息重新连接。如果连接成功，就将前面连接失败的审计记录信息覆盖，以防止恶意用户加密的口令强行重新连接。

DBA 应该根据所有各类用户实行相关的权限管理，即应充分利用“角色”这个机制的方便性对权限进行有效的管理。

（2）DBA 的安全性策略。

当系统规模较小时，只需要一个 DBA，则系统安全管理员（SSA）也是 DBA。当系统规模很大时，系统拥有多个 DBA，这时两者是分开的。安全管理员将相关管理权限分成几个组，然后将不同的角色授予相应的 DBA。

当创建数据库后，立即更改有管理权限的 sys 和 system 用户的口令，防止非法用户访问数据库。当作为 sys 和 system 用户连入数据库后，用户有强大的权限用各种方式对数据库进行改动。

只有 DBA 能用管理权限连入数据库，并保证只有 DBA 能作 SYSDBA 角色的成员，

因为 SYSDBA 可以没有任何限制地操作和恢复数据库及数据库对象。

3．数据保护

数据库的数据保护主要是数据库的备份，当计算机的软硬件发生故障时，利用备份进行数据库恢复，以恢复破坏的数据库文件或控制文件或其他文件。另一种数据保护就是日志，Oracle 数据库实例都提供日志，用来记录事务对数据库的更新操作的文件，每个事务开始的标记、结束的标记和更新操作均作为日志文件中的一个日志记录存储在日志文件中，以便恢复数据库使用。再一个就是控制文件的备份，它一般用于存储数据库物理结构，包含了数据库名、数据库数据文件和日志文件的名字和位置、数据库建立日期。每一次 Oracle 数据库的实例启动时，它的控制文件用于标识数据库和日志文件，当着手数据库操作时它们必须被打开。当数据库的物理组成更改时，Oracle 自动更改该数据库的控制文件。数据恢复时，也要使用控制文件。

Oracle 数据库的备份日常工作中，数据库的备份是数据库管理员必须不断进行的一项工作，数据库的备份主要有冷备份、热备份和逻辑备份。冷备份首先要用 shutdown immediate 命令来关闭数据库，然后在操作系统复制所有的数据库文件，包括数据文件、控制文件、参数文件和密码文件等（要想获取数据库文件信息，可通过查询数据字典动态视图获取：V ＄DATAFILE ，V ＄CONTROLFILE，V ＄LOGFILE 和 V ＄TABLESPACE 视图）。最后用 startup open 命令打开数据库。逻辑备份是使用 Oracle 提供的操作系统工具 Export、Import 将数据库中的数据卸载、装入。在每一个 Oracle 数据库中，可以使用 Export 命令将数据库中的数据备份成一个二进制的操作系统文件，该文件格式为 Dmp（export dump file）。卸载的文件可以使用另一个操作系统命令 Import 重新装入到另一个数据库中。热备份即正在运行数据库的备份，这时数据库必须设置为 Archivelog 模式，在线 Redo 日志文件必须是归档的，或者开启了自动归档进程。热备份可在表空间或数据文件级备份，备份时间短，备份时数据库仍可使用，可达到秒级恢复（恢复到某一时间上），可对几乎所有数据实体恢复，恢复是快速的，在大多数情况下可在数据仍工作时恢复。但是，热备份不能出错，否则后果严重；并且，若热备份不成功，所得结果不可用于时间点的恢复；还有，维护困难，所以要特别仔细小心，不允许“以失败而告终”。

Oracle 数据库的恢复有了上述几种备份方法，即使计算机发生故障，如介质损坏、软件系统异常等情况时，也不必惊慌失措，可以通过备份进行不同程度的恢复，使 Oracle 数据库系统尽快恢复到正常状态。

（1）数据文件损坏。

这种情况可以用最近所做的数据库文件备份进行恢复，即将备份中的对应文件恢复到原来位置，重新加载数据库。

（2）控制文件损坏。

若数据库系统中的控制文件损坏，则数据库系统将不能正常运行，那么，只需将数据库系统关闭，然后从备份中将相应的控制文件恢复到原位置，重新启动数据库系统即可。

(3) 整个文件系统损坏。

在大型的操作系统中,如 UNIX,由于磁盘或磁盘阵列的介质不可靠或损坏是经常发生的,这将导致整个 Oracle 数据库系统崩溃,这种情形只能将磁盘或磁盘阵列重新初始化,去掉失效或不可靠的坏块,重新创建文件系统,利用备份将数据库系统完整地恢复,启动数据库系统。

4. Oracle 审计机制

利用 Oracle 数据库系统的审计功能,同样可以监视和记录所选择用户的活动情况。在默认状况下,系统为了节省资源、减少 I/O 操作,数据库的审计功能是关闭的。为了启动审计功能,必须修改参数文件,将数据库审计控制参数 audit_trail 改为 true。Oracle 数据库的审计级别共有三种:语句级审计、权限级审计和实体级审计。语句级审计表示只审计某种类型的 SQL 语句,不指定结构或对象;权限级审计表示只审计执行相应动作的系统特权的使用状况;实体级审计表示只对一指定模式上的实体的指定语句的审计。

5.4 应用实例

5.4.1 Windows 账号安全管理

在操作系统安全管理中,账号安全管理是建立一个安全的系统环境非常重要且最基础的一步,前面介绍操作系统安全理论知识也提到,用户账号不适当的安全问题是攻击侵入系统的主要手段之一,做好账号安全管理能有效解决和防范操作系统安全问题。

下面通过实例说明 Windows XP 操作系统下账号安全管理方法。

1. 重命名和禁用默认的账户

第 1 步:查询所有用户的账号。

(1) 在 Windows XP 操作系统中,右击桌面"我的电脑"图标,选择"管理"菜单项,打开"计算机管理"窗口,如图 5-6 所示。



图 5-6 "计算机管理"对话框

（2）在左边列表中找到并展开“本地用户和组”，单击“用户”选项，可以查询到系统中的账户。

第 2 步：禁用“Guest(来宾)”账户。

在如图 5-6 所示“计算机管理”对话框中，右击“Guest”账户选择“属性”命令，在“Guest 属性”对话框中，勾选“账户已停用”选项，然后单击【确定】按钮，禁用 Guest 账户，如图 5-7 所示。

第 3 步：创建新账户。

在图 5-6 所示“计算机管理”窗口中，“操作”菜单中选择“新用户”创建新账户，在出现的“新用户”对话框中，输入用户名并设置密码，如图 5-8 所示。注意：密码根据系统版本不同会有不同要求，另外图 5-8 给出用户名仅为示例，可根据实际要求做不同调整。



图 5-7　Guest 账户属性对话框



图 5-8　创建“新用户”对话框

第 4 步：添加新账户属性。

（1）在图 5-6 所示“计算机管理”窗口中，右击第 3 步创建的新账户“zzw”，选择“属性”，然后在出现的账户属性窗口中，单击“隶属于”选项卡，如图 5-9 所示。

（2）在图 5-9 中，单击【添加】按钮，出现如图 5-10 所示的“选择组”对话框。



图 5-9　账户属性对话框



图 5-10　“选择组”对话框

(3) 单击图 5-10 中的【高级】按钮，在“选择组”窗口中单击【立即查找】按钮，点选列表中的“Administrators”选项，如图 5-11 所示。



图 5-11　添加新账户属性

(4) 单击【确定】按钮。随后连续单击【确定】按钮，回到如图 5-6 所示“计算机管理”窗口中，完成将新账户加入管理组。

第 5 步：登录新账户。

重新启动计算机，以新建的 zzw 账户登录系统。按照上述步骤在“计算机管理”窗口中停用“Administrator”账户。

2. 设置密码策略

(1) 尽管绝对安全的密码是不存在的，但是可以实现相对安全的密码。在“开始”菜单中打开“运行”对话框，输入“secpol. msc”打开“本地安全设置”窗口，展开“账户策略”，单击“密码策略”，右侧有 6 项关于密码的设置策略，如图 5-12 所示。通过这些策略的配置，就可以建立完备密码策略，这样密码就可以得到最大限度的保护。

(2) 在“账户锁定策略”中，如图 5-13 所示，可对“复位账户锁定计数器”、“账户锁定时间”和“账户锁定阈值”3 项策略进行设置。

(3) Windows XP 登录密码存放在系统的 C:\WINDOWS\system32\config 下的 sam 文件中，如图 5-14 所示。sam 文件就是存放账号和密码的数据库文件。当登录系统时，系统会自动和 sam 进行比较，如果发现此账号和密码与 sam 文件中的加密数据符合，用户就会顺利登录，如果错误则无法登录。

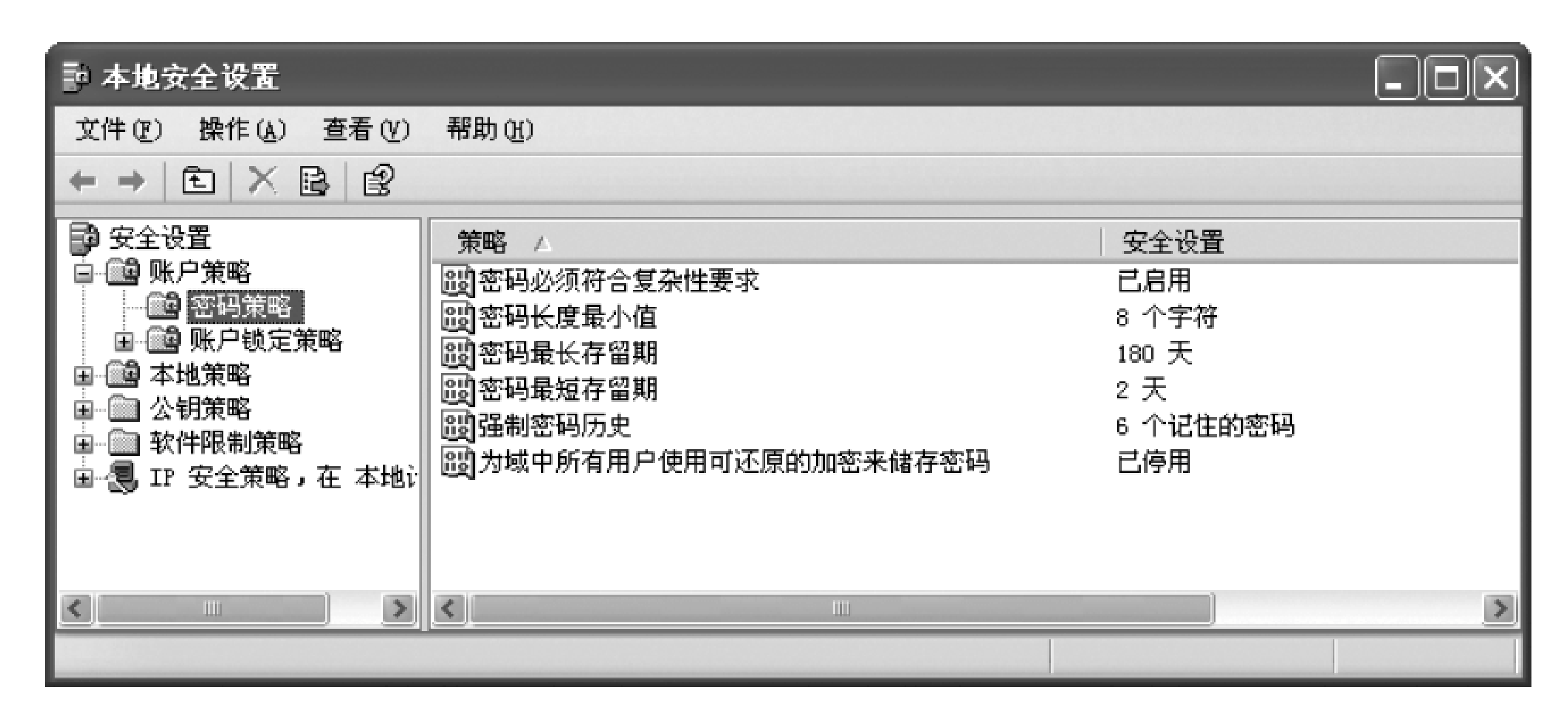


图 5-12　设置“密码策略”对话框



图 5-13　“账户锁定策略”对话框

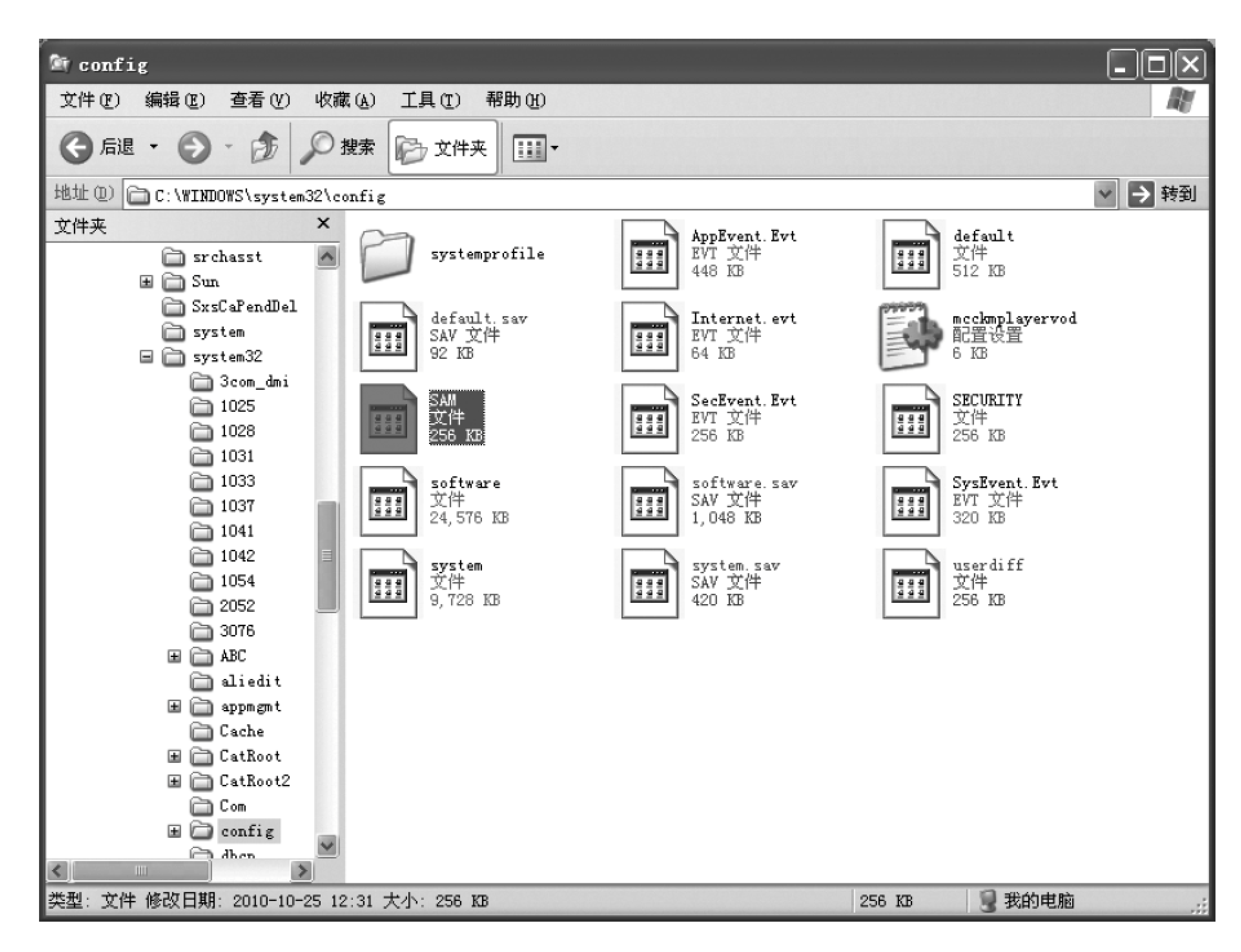


图 5-14　登录密码存储位置窗口

3. 双重加密账户

虽然为账户设置了复杂的密码,但密码总有被破解的可能。此时可以为账户设置双重加密。

第 1 步:在计算机“开始”菜单中打开“运行”对话框,输入“syskey”,打开“保证 Windows XP 账户数据库的安全”对话框,如图 5-15 所示。

第 2 步:在图 5-15 选中“启用加密”选项,单击【确定】按钮,这样程序就对账户完成了双重加密,不过这个加密过程对用户来说是透明的。注意:该项操作是不可逆,一旦启用加密则不可以禁用。

备注:如果想更进一步体验这种双重加密功能,那么可以在图 5-15 中单击【更新】按钮,打开“启动密码”对话框,如图 5-16 所示,有“启动密码”和“系统产生的密码”两个选项。

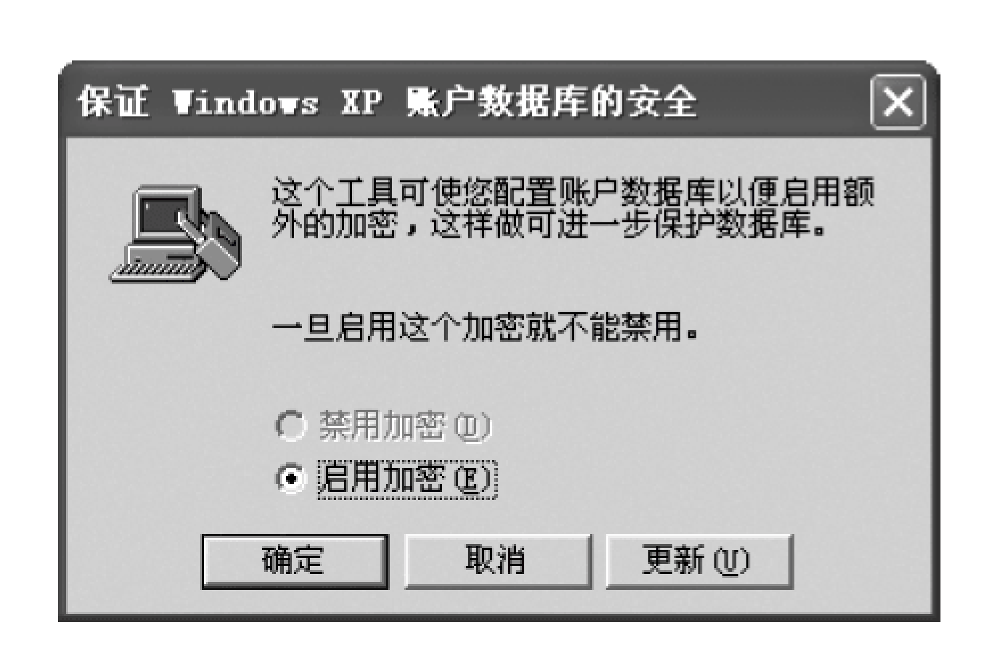


图 5-15 “保证 Windows XP 账户数据库的安全”对话框

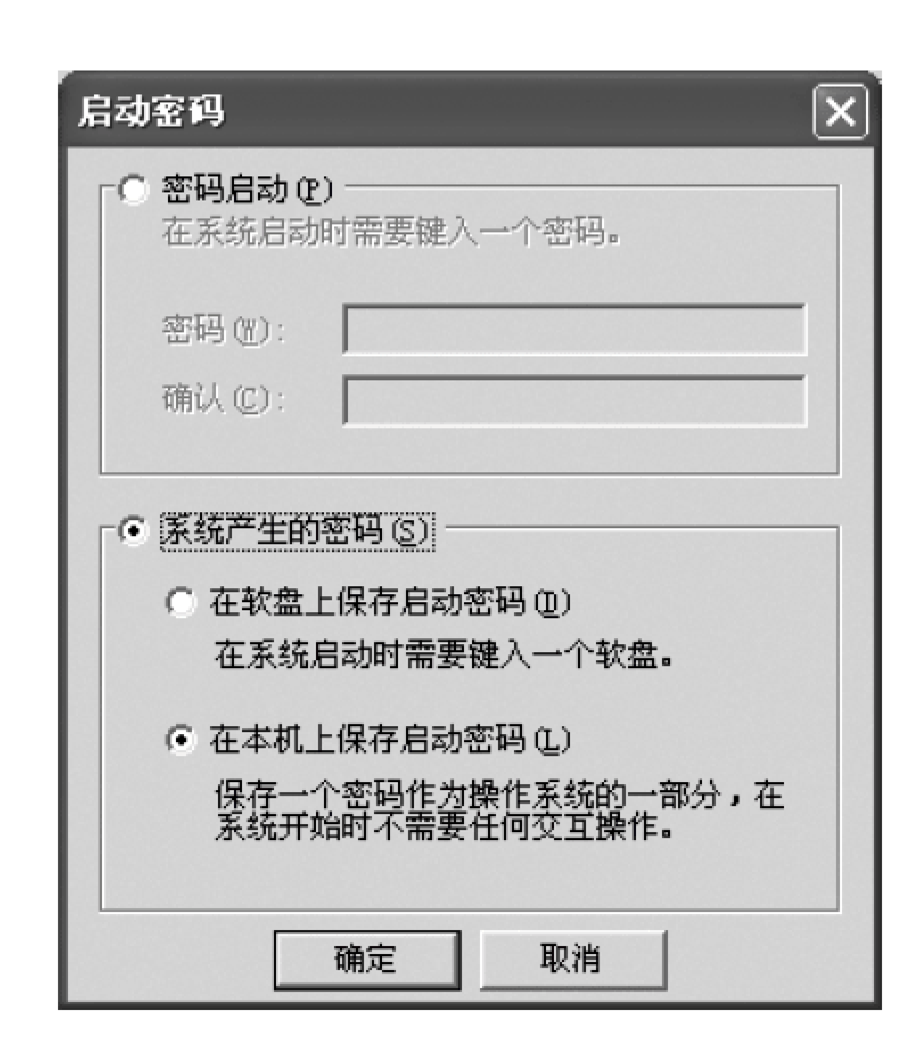


图 5-16 “启动密码”对话框

如果选择“密码启动”,那么需要自己设置一个密码,这样在登录 Windows XP 之前需要先输入这个密码,然后才能选择登录的账户。

如果选择“系统产生的密码”,那么又有两个选项,系统的默认选项是“在本机上保存启动密码”,如果选择该选项,那么程序仅在后台完成加密过程,在用户登录时不要求输入任何密码,因为密码就保存在计算机的内部。如果对安全要求很高,那么可以选择“在软盘上保存启动密码”,单击【确定】按钮之后会提示在软驱里放入一张软盘,创建完毕后会在软盘上生成一个 StartKey.Key 文件,以后每次启动系统时必须放入该软盘才能登录,此时相当于系统有了一张可以随身携带的钥匙盘。

5.4.2 Oracle 数据安全备份与恢复

如果对数据库进行了周期性备份,则在数据丢失时用户可以将存储的重要信息应用到最新的备份中,从而恢复数据库的当前状态。Oracle 使用户能够还原一个较早的备份和仅应用某些重做数据,从而将数据库恢复到一个较早的时间点,这样就能减少数据库系

统遇到问题时的损失。下面就通过实例来介绍 Oracle 9i 的数据安全备份与恢复操作。

1. 本机数据库数据备份

第 1 步：打开 Windows 操作系统中自带程序“命令提示符”窗口。

第 2 步：输入语句“exp med/med@med file=c:\med.dmp owner=med”，此命令语句的格式为“exp 数据库用户名/数据库密码@数据库实例名 file=导出的文件名和路径 owner=数据库用户名”(备注：命令语句中数据库用户名为“med”，数据库密码为“med”，数据库实例名为“med”，导出的文件名和路径为“c:\med.dmp”，可以根据实际情况更改语句)。

第 3 步：命令语句输入完毕后，按 Enter 键，即可对本机数据库进行备份，如图 5-17 所示。

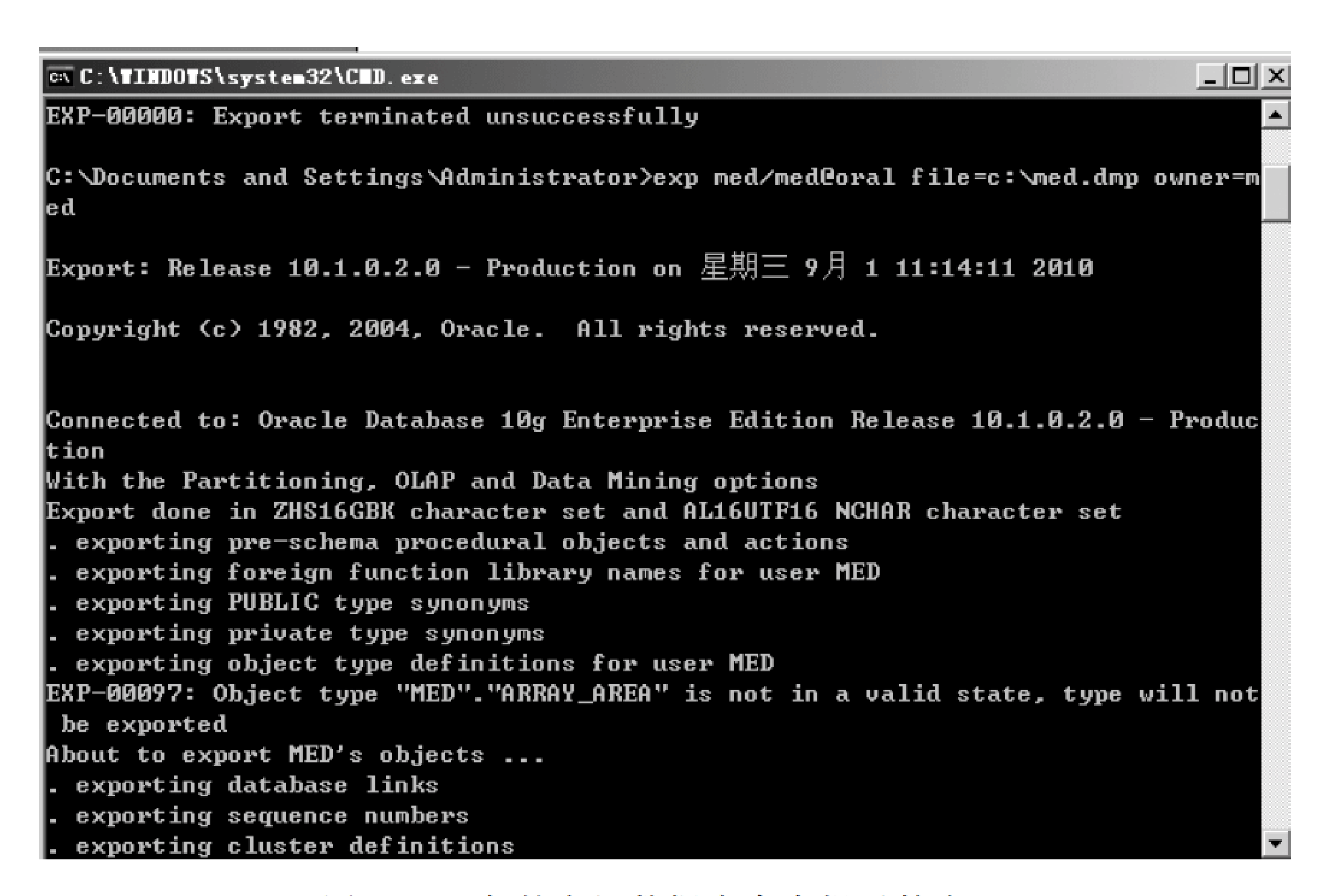


图 5-17　备份本机数据库命令提示符窗口

2. 其他服务器上的数据库数据备份

第 1 步：配置服务。

(1) 打开操作系统中安装好的 Oracle 数据库“Configuration and Migration Tools”菜单，单击“Net Configuration Assistant”打开服务配置对话框，如图 5-18 所示。

(2) 选中图 5-18 中“本地 Net 服务名配置”选项，单击【下一步】按钮，跳转到下一步，进行服务器名配置。

(3) 选中“添加”选项，如图 5-19 所示，单击【下一步】按钮。

(4) 选择需要的数据库或服务版本，如图 5-20 所示，单击【下一步】按钮。

(5) 输入服务名“med”，如图 5-21 所示，单击【下一步】按钮。

(6) 选择所要配置服务的协议，如图 5-22 所示，单击【下一步】按钮。

(7) 如图 5-23 所示，输入服务器 IP，单击【下一步】按钮。



图 5-18　Oracle 9i 服务配置对话框



图 5-19　Oracle 9i 服务名配置对话框



图 5-20　选择服务版本设置对话框



图 5-21　服务名输入对话框



图 5-22　服务协议对话框



图 5-23　服务 IP 地址输入设置

（8）当前面的设置完成以后会询问是否需要测试连接数据库，如果需要则选择“是，进行测试”继续完成接下来的步骤。

（9）连接测试不成功会提示输入登录用户名和密码，按照前面给出的信息输入，如图 5-24 所示更改密码，单击【确定】按钮。



图 5-24　更改登录对话框

（10）当连接成功后会提示测试成功，单击【下一步】按钮，输入服务名“med”，如图 5-25 所示，单击【下一步】按钮会提示是否配置另一个 Net 服务名，如图 5-25 所示。



图 5-25　重新配置服务名对话框

（11）在图 5-25 中选则“否”选项，然后单击【下一步】按钮，提示服务名配置完毕，如图 5-26 所示。

（12）在图 5-26 中单击【下一步】按钮后会跳转回到图 5-18 对话框中，单击【完成】按钮。

第 2 步：打开 Windows 操作系统中自带程序“命令提示符”窗口。



图 5-26　“服务名配置完毕”对话框

第 3 步：输入命令“exp med/med@med file=c:\med.dmp owner=med；exp”。然后按 Enter 键，即可导出数据库，如图 5-27 所示。

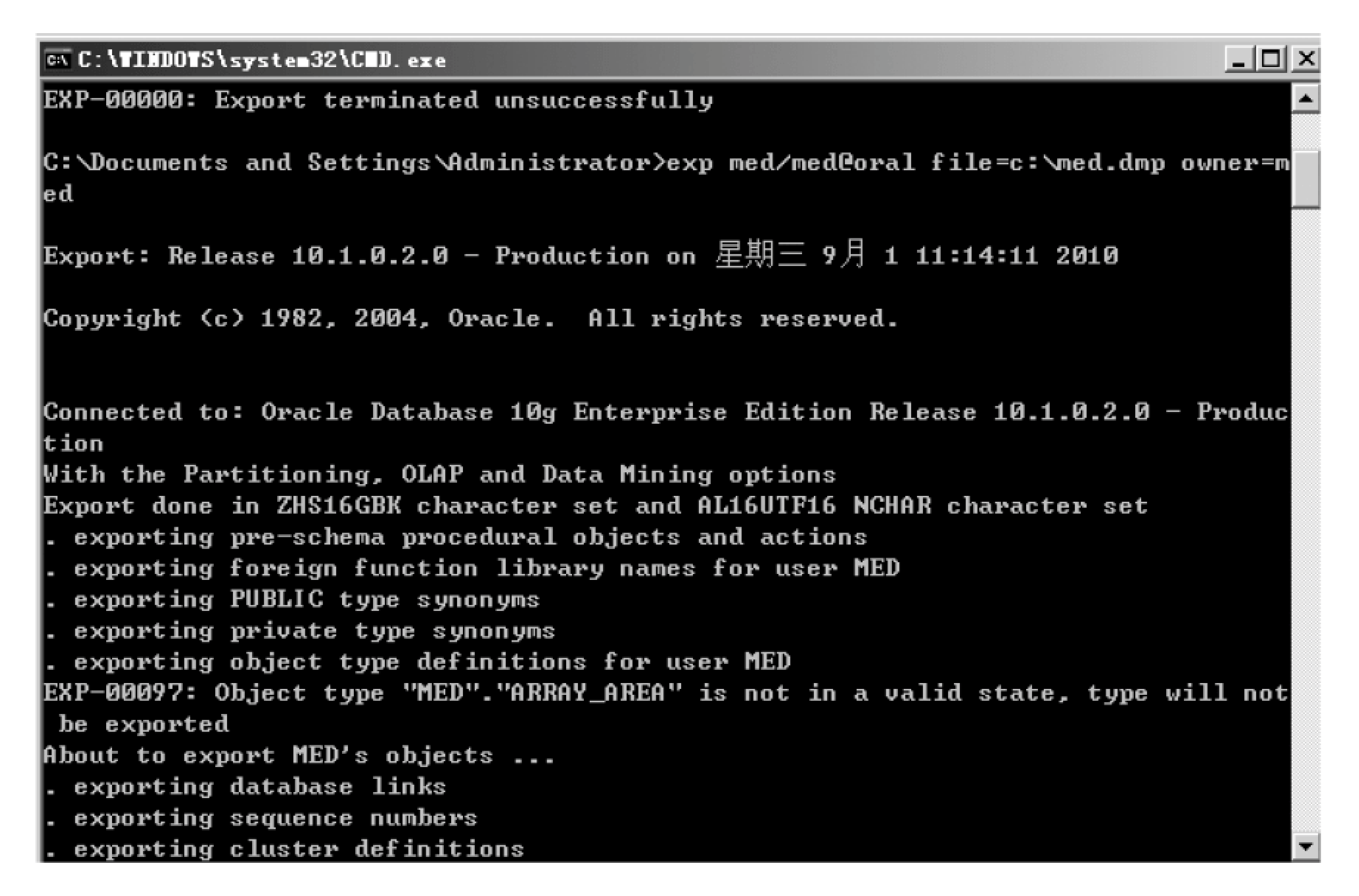


图 5-27　导出数据库命令窗口

3. 还原数据备份

第 1 步：创建实例。

(1) 在 Windows 桌面上通过“开始”按钮选择 Oracle 数据库“Configuration and Migration Tools”→“Database Configuration Assistant”菜单命令，打开“数据库”对话框，如图 5-28 所示，单击【下一步】按钮。

(2) 选择数据库模板“Data Warehouse”选项，如图 5-29 所示，单击【下一步】按钮。



图 5-28　“数据库”对话框



图 5-29　“数据库模板”选择对话框

(3) 如图 5-30 所示填写数据库名“med”，SID“med”，单击【下一步】按钮。

(4) 选择“专用服务器模式”如图 5-31 所示，单击【下一步】按钮。



图 5-30 “数据库标识”对话框



图 5-31 数据库默认操作模式对话框

(5) 在如图 5-32 所示的初始化参数对话框中选择“字符集”选项卡,在“数据库字符集”中选择“从字符集列表中选择”,将字符编码设置为“UTF8”,单击【下一步】按钮。

(6) 完成第(5)个操作以后,出现“数据库存储”窗口,直接单击【下一步】按钮,会显示创建选项对话框,如图 5-33 所示,勾选“创建数据库”,然后单击【完成】按钮,完成实例的创建。



图 5-32 “初始化参数”对话框

图 5-33 “创建选项”对话框

第 2 步：在操作系统中单击左下角的“开始”图标，选择“运行”，输入“sqlplus”命令，打开 sqlplus 窗口。

第 3 步：创建用户。

在 sqlplus 窗口中输入命令语句“create user med identified by med”，然后按 Enter 键。此语句格式为“create user 数据库用户名 identified by 数据库实例名”，其中数据库

用户名为“med”，数据库实例名为“med”，都可以根据实际情况做调整。

第 4 步：授权。

在 sqlplus 窗口中输入命令语句“grant dba to med”，然后按 Enter 键，完成后如图 5-34 所示。此语句格式为“grant 连接角色 to 数据库用户名”，其中系统角色为“dba”，数据库用户名为“med”，都可以根据实际情况做调整。

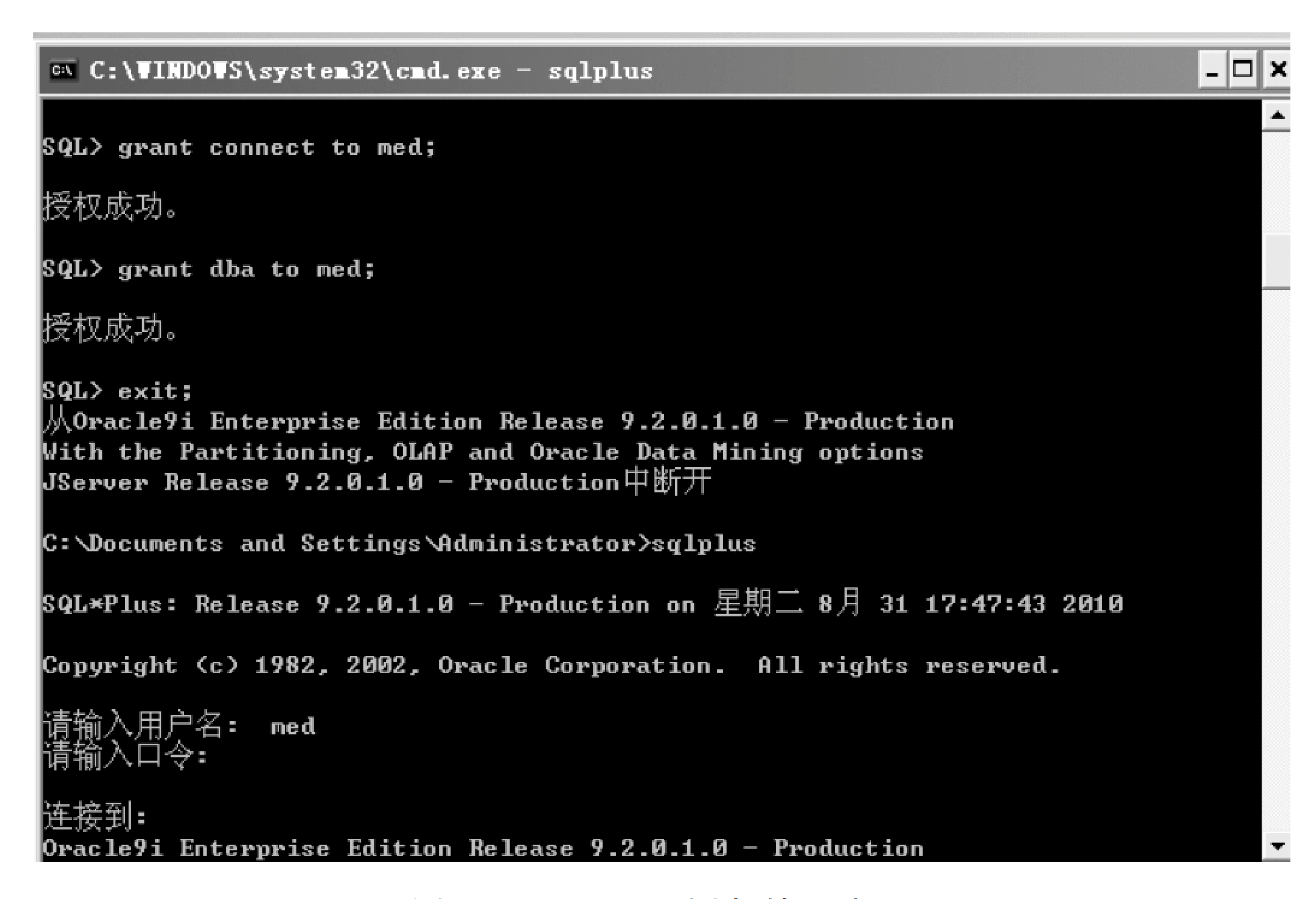


图 5-34　sqlplus 语句输入窗口

第 5 步：打开 Windows 操作系统中自带程序“命令提示符”窗口。

第 6 步：输入语句“imp userid=med/med@med fromuser=med touser=med file=(c:\med.dmp)”，此命令语句的格式为“imp userid=数据库用户名/数据库密码@数据库实例名 fromuser=数据库用户名 touser=数据库用户名 file=(导出的文件名和路径)”。然后按 Enter 键，即可还原数据库。

5.5　案例讨论

31 岁的程某是名牌大学毕业，经过多年打拼已是 X 公司资深软件研发工程师，聪明的头脑让他获得领导的赏识，可谓年轻有为，前途无量。程某对工作很是勤奋，工作上电信业务是他的强项，经过长时间的业务接触，他对电信公司网络了如指掌。在一次偶然的机会里，程某无意间访问到了充值卡的信息。程某看到这些充值卡后开始动起了歪脑筋。

程某告诉朋友赵某，这正是发财的一个机会。他们梦想自己过上优越的生活，坐好车、住好房、数钱。为了让自己的计划顺利实施，赵某、程某做了分工，程某负责盗窃、赵某负责销售。程某偷偷潜入了运营商网络，进入电信充值中心数据库，充值中心数据库有很多过期的充值卡，程某破解出密钥，修改充值卡的时间和金额，把“已充值”状态改为“未充值”。在 4 个月的作案过程中，程某共计牟利 400 多万元，后来由于在修改过程中出现了未置位时间，被买到充值卡的用户举报到客服中心，经过内部层层追查才发现了程某。

本章两个案例都与数据库有关，比较分析两则案例的相同之处，讨论如何规范数据库管理人员工作行为？如何才能有效保护数据库的安全？

归纳总结

1. 归纳针对操作系统和数据库系统的安全威胁有哪些相同之处与不同之处。

2. 归纳操作系统面临的安全威胁，总结保护操作系统安全应使用什么安全技术与措施。

3. 归纳数据库系统面临的安全威胁，总结保护数据库系统安全应使用什么安全技术与措施。

思考与实践

思考题

1. 什么是系统软件？系统软件和应用软件有什么不同之处？
2. 对于系统软件而言有什么样的安全威胁？
3. 目前较为常见的系统软件有几类？为何这几类系统软件很重要？
4. 在日常的了解与学习中，你还知道几种除本书所提到的操作系统？安全性如何？
5. 你是如何理解数据库系统安全的重要性的？

实践题

1. 根据自己平时所常用的操作系统，创建不同权限的账号，比较其不同点。
2. 建立一个 Access 数据库，并且用不同的方法增强其安全性，同时记录步骤。
3. Oracle 数据库备份有几种不同方法？除了应用实例 5.4.2 给出的方法以外，尝试使用不同的备份方法对数据库进行数据安全备份。

计算机病毒防治技术

学习目标

通过本章的学习，能够——

- 了解计算机病毒的基础知识；
- 了解传统计算机病毒的工作机制和危害；
- 了解互联网时代下典型病毒的工作机制和危害；
- 掌握计算机病毒检测、清除与预防的方法；
- 掌握常用反病毒软件的使用方法。

引导案例

在计算机早已经成为普及工具的那一刻，病毒也开始了“工业化”入侵的进程。自计算机诞生的那天起，病毒就如影随形。随着互联网的不断发展，病毒也不断演变，新型病毒借网络大肆传播并显示出极强的破坏力。在各种病毒肆虐之际，广大用户往往饱受其害，受灾企业更是不计其数。病毒使很多企业网络瘫痪，信息交流完全中断；计算机无法使用，成为一堆高科技的废铁；日常办公回到手工时代，严重的甚至正常运作被迫中止……

病毒/木马背后所带来的巨大的经济利益让计算机系统进入了从所未有的“危险期”。

扫描端口、远程入侵、下载木马等一系列病毒攻击程序早已经成为流水线上的固定步骤，迈入了“工业自动化”阶段，而抓取“肉鸡”的效率也取决于用于发起攻击的计算机性能和网络带宽。

新的病毒和被快速模仿的变种病毒以出其不意的速度疯狂地袭击着每一个它们可以找到漏洞的地方，计算机蓝屏、频繁重启、网络瘫痪，像是魔鬼一样开始在黑暗里和我们斗争。而“黑客”正在幕后策划着如何将这些病毒的价值最大化，让自己赚到更多的钱。

他们毫不在乎成千上万人的生活和工作被这些病毒所干扰，因为只有我们的损失才能变成他们的财富。

病毒种类越来越多，影响面越来越大，破坏性越来越强。依据国内著名病毒厂商报告，2009 年其免费杀毒下载软件共截获新增病毒和木马超过 2 千万个，比 5 年前的新增病毒数量增长了近 400 倍。下面是近些年的相关数据和事件。

截至 2003 年，活体计算机病毒达 14 000 种，网络病毒有更大的破坏性（占 52%）；
1988 年的莫里斯事件（UNIX/E-mail）：6000 台计算机感染，损失 9000 万美元；
1998 的 CIH 病毒（系统程序和硬盘数据）：2000 万台计算机感染；
1999 年的梅丽莎案件（Window/E-mail）：8000 万台计算机感染；
2000 年的爱虫病毒：1200 万台计算机感染，损失几十亿美元；
2001 年的红色代码、尼姆达病毒：蠕虫/木马/黑客；
2002 年的求职信病毒；
2003 年的冲击波病毒；
2004 年的震荡波（Sasser）病毒；
2006 年的"熊猫烧香（Nimaya）"病毒；
2007 年的"网游大盗"病毒；
……

6.1 计算机病毒概述

本节主要介绍计算机病毒的定义及特点，并在此基础上讲述计算机病毒的结构、分类、命名规则，以及病毒主要有哪几种入侵方式等相关问题。

6.1.1 计算机病毒的定义与危害

1. 计算机病毒的定义

在《中华人民共和国计算机信息系统安全保护条例》中计算机病毒（computer virus）被明确定义为"编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码"。

通俗地讲，病毒就是利用计算机软件与硬件的缺陷或操作系统的漏洞，由被感染机内部发出的破坏计算机数据并影响计算机正常工作的一组指令集或程序代码。

计算机病毒与生物病毒一样，由自身病毒体（病毒程序）和寄生体（宿主 HOST）组成。所谓感染或寄生，是病毒将其自身嵌入到宿主指令序列中。寄生体为病毒提供一种生存环境，是一种合法程序。当病毒程序寄生于合法程序之后，病毒就成为程序的一部分，并在程序中占有合法地位，随后就会随着合法程序在计算机中运行。为了增强活力，病毒程序通常寄生于一个或多个被频繁调用的程序中。

2. 计算机病毒的危害

（1）病毒激发对计算机数据信息造成直接破坏。

大部分病毒的破坏手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的"垃圾"数据改写文件、破坏 CMO 设置等。

（2）占用磁盘空间，对信息进行破坏。

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒的一般侵占方式是

由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些DOS功能进行传染，这些DOS功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用部位去，所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。

(3) 抢占系统资源。

大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。除占用内存外，病毒还抢占中断，干扰系统运行。

(4) 影响计算机运行速度。

主要表现在：①病毒为了判断传染激发条件，总要对计算机的工作状态进行监视。②有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的CPU指令再执行，而病毒运行结束时再用一段程序对病毒重新加密。这样CPU额外执行数千条以至上万条指令。③病毒在进行传染时同样要插入非法的额外操作，特别是传染软盘时不但计算机速度明显变慢，而且软盘正常的读写顺序被打乱，发出刺耳的噪声。

(5) 不可预见的危害。

计算机病毒与其他软件的一大差别是病毒的无责任性，很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析大量病毒后发现绝大部分病毒都存在不同程度的错误。错误病毒的另一个主要来源是变种病毒。有些初学计算机者尚不具备独立编制软件的能力，出于好奇或其他原因修改别人的病毒，造成错误。大量含有未知错误的病毒扩散传播，其后果是难以预料的。

(6) 兼容性对系统运行的影响。

病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

(7) 给用户造成严重的心理压力。

据有关计算机销售部门统计，计算机用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的60%以上。经检测确实存在病毒的约占70%，另有30%情况只是用户怀疑，而实际上计算机并没有病毒。

6.1.2 计算机病毒的产生与发展

1. 计算机病毒的起源

计算机病毒是紧随着计算机而诞生的。1949年计算机之父冯·诺依曼在《复杂自动机组织论》(Complex auto matic machine theory of organization)一书提出了计算机病毒的基本概念——“一部事实上足够复杂的机器能够复制自身”。这种说法在当时让人感到比较离谱，但一些黑客却对此深为敏感，并在暗地里悄悄开始了程序“自我复制”的研究，计算机病毒发展史也从此揭开了序幕。

对于计算机病毒最初的来源，计算机病毒学界有三种重要的“起源说”，即“恶作剧论”、“加密陷阱论”和“游戏程序起源说”。

（1）恶作剧论。

持这种观点的人认为：计算机病毒源于一些计算机爱好者的恶作剧。23年前，美国奈尔大学的罗伯特·莫里斯（Robert Morris）因编写蠕虫病毒程序肇事后，却被称为软件奇才，一些公司出高薪争相聘用他。蠕虫受害者在分析报告中客观地指出：当蠕虫程序混入网络骗取口令之后，蠕虫程序就已经获取了系统用户的特权，可以读取被保护的数据，蠕虫因此而具备了进行严重破坏活动的能力。但是蠕虫现在还没有做这些，它造成的伤害仅仅是使计算机运转变缓慢。莫里斯在编写蠕虫程序时，单枪匹马地破译了采用DES对称密码的口令。对DES密码，IBM公司曾组织了一些密码专家，花费了几周时间未能破译。莫里斯的技术能力令人震惊。他成了最有名的攻击者，他的超人能力引起广泛关注，哈佛大学就专门授予他超级用户的特权。人们曾普遍认为这些编病毒的年轻人是一群“可畏的恶作剧制作者”，不可小视。

（2）加密陷阱论。

这种观点认为计算机病毒起源于软件加密技术。软件产品是一种知识密集的高科技产品。软件产品的研制耗资巨大，而且生产效率很低，但复制软件却异常的简单。由于各种原因，社会未能对软件产品提供有力的保护，大量存在非法复制和非法使用的情况，因而严重地损害了软件产业的利益。为了保护软件产品，防止非法复制和非法使用，软件产业发展了软件加密技术，使软件产品只能使用，不能复制。

早期的加密技术是自卫的，它可以使程序锁死，使非法用户无法使用，或使磁盘“自杀”，防止非法用户重复破译。后来随着加密与破译技术的激烈对抗，软件加密由自卫性转化为攻击性，于是就产生了计算机病毒。著名的巴基斯坦病毒C-Brain，是世界上唯一给出病毒制造者姓名和地址的病毒，其目的就是跟踪软件的非法用户。

（3）游戏程序起源说。

持这种观点的人认为：计算机病毒起源于游戏程序。20世纪60年代初，美国麻省理工学院的一些青年研究人员，在做完工作后，利用业余时间玩一种他们自己创造的计算机游戏。做法是某个人编制一段小程序，然后输入到计算机中运行，并销毁对方的游戏程序。而这也可能就是计算机病毒的雏形，这个小程序就是著名的“磁芯大战”。

2. 计算机病毒制造者的目的

从计算机病毒制造者的角度来看，他们编写病毒的主要目的是：

（1）报复某人或某个集体甚至整个社会。

（2）炫耀技术。

（3）盗取账号以获得非法收益。

（4）为其他流氓网站服务，强制修改你的首页以获得佣金。

（5）直接在网上挂卖给其他有兴趣的人，获得收益。

3. 计算机病毒的发展

在计算机病毒的发展史上，病毒的出现是有规律的，一般情况下一种新的病毒技术出现后，病毒迅速发展，接着反病毒技术的发展会抑制其流传。操作系统升级后，病毒也会调整为新的方式，产生新的病毒技术。目前计算机病毒发展可以分为 10 个阶段。

（1）DOS 引导阶段。

1987 年，计算机病毒主要是引导型病毒，具有代表性的是“小球”和“石头”病毒。当时的计算机硬件较少，功能简单，一般需要通过软盘启动后使用。引导型病毒利用软盘的启动原理工作，它们修改系统启动扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读写中断，影响系统工作效率，在系统存取磁盘时进行传播；1989 年，引导型病毒发展为可以感染硬盘，典型的代表有“石头 2”病毒。

（2）DOS 可执行阶段。

1989 年，可执行文件型病毒出现，它们利用 DOS 系统加载执行文件的机制工作，代表为“耶路撒冷”、“星期天”病毒，病毒代码在系统执行文件时取得控制权，修改 DOS 中断，在系统调用时进行传染，并将自己附加在可执行文件中，使文件长度增加；1990 年，发展为复合型病毒，可感染. COM 和. EXE 文件。

（3）伴随型阶段。

1992 年，伴随型病毒出现，它们利用 DOS 加载文件的优先顺序进行工作，具有代表性的是“金蝉”病毒。伴随型病毒感染. EXE 文件时根据算法产生. EXE 文件的伴随体，具有同样的名字和不同的扩展名（. COM），例如：XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入. COM 文件并不改变. EXE 文件，当 DOS 加载文件时，伴随体优先被执行到，病毒就取得控制权。这类病毒的特点是不改变原来的文件内容、日期及属性的，解除病毒时只要将其伴随体删除即可。

（4）幽灵、多形阶段。

1994 年，随着汇编语言的发展，实现同一功能可以用不同的方式进行完成，这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点，每感染一次就产生不同的代码。例如“一半”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏在解码前的数据中，查解这类病毒就必须能对这段数据进行解码，加大了查毒的难度。多形型病毒是一种综合性病毒，它既能感染引导区又能感染程序区，多数具有解码算法，一种病毒往往要两段以上的子程序方能解除。

（5）生成器、变体机阶段。

1995 年，在汇编语言中，一些数据的运算放在不同的通用寄存器中，可运算出同样的结果，随机地插入一些空操作和无关指令，也不影响运算的结果，这样，一段解码算法就可以由生成器生成，当生成器的生成结果为病毒时，就产生了这种复杂的“病毒生成器”，而变体机就是增加解码复杂程度的指令生成机制。这一阶段的典型代表是“病毒制造机”VCL，它可以在瞬间制造出成千上万种不同的病毒，查解时就不能使用传统的特征识别法，需要在宏观上分析指令，解码后查解病毒。

（6）网络蠕虫阶段。

1995 年，随着网络的普及，病毒开始利用网络进行传播，它们只是以上几代病毒的改

进。在非 DOS 操作系统中,“蠕虫”是典型的代表,它不占用除内存以外的任何资源,不修改磁盘文件,利用网络功能搜索网络地址,将自身向下一地址进行传播,有时也在网络服务器和启动文件中存在。

(7) 视窗阶段。

1996 年,随着 Windows 和 Windows 95 的日益普及,利用 Windows 进行工作的病毒开始发展,它们修改(NE 或 PE)文件,典型的代表是 DS. 3873,这类病毒的机制更为复杂,它们利用保护模式和 API 调用接口工作,解除方法也比较复杂。

(8) 宏病毒阶段。

1996 年,随着 Windows Word 功能的增强,使用 Word 宏语言也可以编制病毒,这种病毒使用类 Basic 语言,编写容易,感染 Word 文档等文件,在 Excel 和 AmiPro 出现的相同工作机制的病毒也归为此类,由于 Word 文档格式没有公开,这类病毒查解比较困难。

(9) 互联网阶段。

1997 年,随着因特网的发展,各种病毒也开始利用因特网进行传播,一些携带病毒的数据包和邮件越来越多,如果不小心打开了这些邮件,计算机就有可能中毒。

(10) 邮件炸弹阶段。

1997 年,随着万维网上 Java 的普及,利用 Java 语言进行传播和资料获取的病毒开始出现,典型的代表是 JavaSnake 病毒,还有一些利用邮件服务器进行传播和破坏的病毒,例如 Mail-Bomb 病毒,它会严重影响因特网的效率。

4. 新一代计算机病毒的特点

随着互联网的发展与计算机技术的进步,计算机病毒形式及传播途径日趋多样化,主要有以下特点:

(1) 病毒技术日趋复杂化。

病毒制造者充分利用计算机软件的脆弱性和互联网的开放性,不断发展计算机病毒技术,朝着能对抗反病毒手段和有目的方向发展,使得病毒的花样不断翻新,编程手段越来越高,防不胜防。例如,利用生物工程学的“遗传基因”原理编写的“病毒生产机”软件,该软件无须病毒编写者绞尽脑汁地编写程序,便会轻易地自动生产出大量的主体构造和原理基本相同的“同族”新病毒。利用军事领域“集束炸弹”原理编写的“子母弹”病毒,该病毒被激活后就会像“子母弹”一样,分裂出多种类型的病毒来分别攻击并感染计算机内不同类型的文件。

(2) 互联网成为计算机病毒的主要传播途径。

计算机病毒最早只通过文件复制传播,当时最常见的传播媒介是软盘和盗版光碟。随着计算机网络的发展,目前计算机病毒可通过计算机网络利用多种方式(电子邮件、网页、即时通信软件等)进行传播。计算机网络的发展有助于计算机病毒的传播速度大大提高,感染的范围也越来越广。可以说,网络化带来了计算机病毒传染的高效率。

(3) 计算机病毒变形的速度极快。

“震荡波”病毒大规模爆发不久,它的变形病毒就出现了,并且不断更新,从变种 A 到变种 F 的出现,时间不用一个月。在人们忙于扑杀“震荡波”的同时,一个新的计算机病

毒应运而生——“震荡波杀手”，它会关闭“震荡波”等计算机病毒的进程，但它带来的危害与“震荡波”类似：堵塞网络、耗尽计算机资源、随机倒计时关机和定时对某些服务器进行攻击。

（4）隐蔽性越来越强。

2007 年 9 月 14 日，微软安全中心发布了 9 月漏洞安全公告。其中 MS04-028 所提及的 GDI＋漏洞，危害等级被定为“严重”。瑞星安全专家认为，该漏洞涉及 GDI＋组件，在用户浏览特定 JPG 图片的时候，会导致缓冲区溢出，进而执行病毒攻击代码。该漏洞可能发生在所有的 Windows 操作系统上，针对所有基于 IE 浏览器内核的软件、Office 系列软件、微软.NET 开发工具，以及微软其他的图形相关软件等，是有史以来威胁用户数量最广的高危漏洞。基于该漏洞的这类“图片病毒”有可能通过以下形式发作：①群发邮件，附带有病毒的.JPG 图片文件；②采用恶意网页形式，浏览网页中的.JPG 文件，甚至网页上自带的图片即可被病毒感染；③通过即时通信软件 QQ、MSN 等的自带头像等图片或者发送图片文件进行传播。在被计算机病毒感染的计算机中，可能只看到一些常见的正常进程如 svchost、taskmon 等，其实它是计算机病毒进程。“蓝盒子（Worm.Lehs）”、“V 宝贝（Win32.Worm.BabyV）”病毒和“斯文（Worm.Swen）”病毒，都是将自己伪装成微软公司的补丁程序来进行传播的。

（5）利用操作系统漏洞传播。

操作系统是联系计算机用户和计算机系统的桥梁，也是计算机系统的核心，目前应用最为广泛的是 Windows 系列的操作系统。“蠕虫王”、“冲击波”、“震荡波”以及“图片病毒”都是利用 Windows 系统的漏洞，在短短的几天内就对整个互联网造成了巨大的危害。

6.1.3 计算机病毒的特性与结构

1. 计算机病毒的特性

虽然计算机病毒种类繁多、特征各异，但一般都具有以下特性：

（1）可执行性。计算机病毒是一个完整的可执行程序，寄生在其他可执行程序上，因此它享有一切程序所能得到的权力。在病毒运行时，与合法程序争夺系统的控制权。计算机病毒只有当它在计算机内得以运行时，才具有破坏能力。

（2）传染性。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。

（3）破坏性。所有的计算机病毒都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源，其具体情况取决于计算机病毒设计者的目的，但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

（4）潜伏性。潜伏性的第一种表现是病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘里待上很长时间，一旦得到运行机会，就四处繁殖、扩散，继续为害。潜伏性的第二种表现是计算机病毒的内部往往有一种触发机制，触发条件一旦得到满足，就会对系统造成各种破坏。

(5) 隐蔽性。由于隐蔽性,计算机病毒得以在用户没有察觉的情况下很快扩散。大部分的病毒的代码之所以设计得非常短小,就是为了隐藏。病毒一般只有几百或1K字节,所以病毒转瞬之间便可将这短短的几百字节附着到正常程序之中,使人非常不易察觉。

(6) 针对性。计算机病毒一般都是针对于特定的操作系统,例如微软的Windows XP、Vista和Win7。还有针对特定的应用程序,例如微软的Office、IE等,它是通过感染数据库服务器进行传播的,一旦攻击成功,便会发作。

(7) 可触发性。病毒因某个事件或数值的出现,诱使病毒实施感染或进行攻击的特性称为可触发性。病毒既要隐蔽又要维持杀伤力,就必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件,这些条件可能是时间、日期、文件类型或某些特定数据等。

2. 计算机病毒的结构

一个病毒包括引导模块、感染模块、触发模块和破坏模块四个模块。

(1) 引导模块。

引导模块负责将病毒由外存引入内存,使传染模块和发作模块处于活动状态。

目前出现的各种计算机病毒的寄生对象有两种:磁盘引导扇区和特定文件(如.EXE、.COM、.DOC、.HTML等)。

寄生在磁盘引导扇区的病毒引导模块将占有原系统引导程序位置,并把原系统引导程序搬移到一个特定的地方。这样系统一启动,病毒引导模块就会自动地装入内存并获得执行权,然后该引导程序负责将病毒程序的传染模块和发作模块装入内存的适当位置,并采取常驻内存技术以保证这两个模块不会被覆盖,接着对这两个模块设定某种激活方式,使之在适当的时候获得执行权。完成这些工作后,病毒引导模块将系统引导模块装入内存,使系统在带病毒的状态下依然可以继续进行。

寄生在文件中的病毒引导模块通过修改原有文件,使对该文件的操作转入病毒程序引导模块,引导模块将完成把病毒程序的传染模块和发作模块驻留内存及初始化工作,然后把执行权交给原文件,使系统及文件在带毒状态下继续运行。

(2) 感染模块。

感染模块负责实现病毒的感染。感染模块主要功能是:①寻找感染目标;②检查目标中是否存在感染标志或设定的感染条件是否满足;③如果没有感染标志或条件满足,进行感染,将病毒代码放入宿主程序。

(3) 触发模块。

触发模块负责判断计算机病毒触发条件。计算机病毒在传染和发作之前,往往要判断某些特定条件是否满足,满足则传染和发作,否则不传染或不发作,这个条件就是计算机病毒的触发条件。

(4) 破坏模块。

破坏模块负责在触发条件满足的情况下,实现病毒对系统或磁盘上的文件进行破坏,病毒破坏目标和攻击部位主要有系统数据区、文件、内存、系统运行速度、磁盘、CMOS、主

板和网络等。这种破坏可能是显示一串无用的提示信息，也可能用来干扰系统或用户的正常工作，有的病毒会造成系统死机或删除磁盘文件，新型病毒还会造成网络拥塞与瘫痪。

计算机病毒的工作流程如图 6-1 所示。

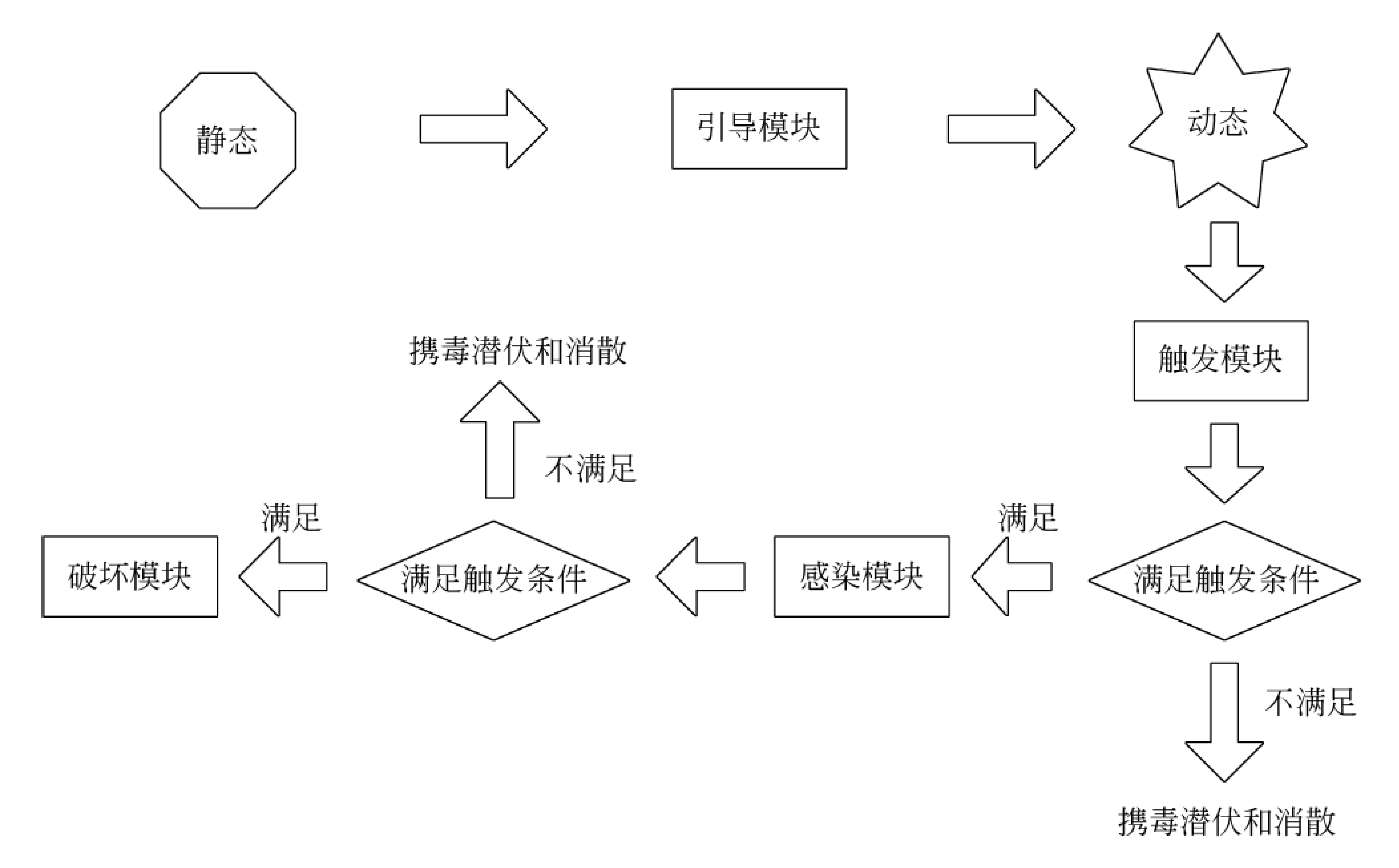


图 6-1　计算机病毒的工作流程示意图

6.1.4　计算机病毒的命名与分类

1. 计算机病毒的命名规则

要有效灭杀病毒，必须从正常文件中区分出病毒，因此需要对病毒的名称有所了解。病毒的命名并没有统一的规定，每个反病毒公司的命名规则都不太一样，但基本都是采用前、后缀法来进行命名的，可以是多个前缀、后缀组合，中间以小数点分隔，一般格式为：[前缀].[病毒名].[后缀]。

病毒前缀是指一个病毒的种类，常见的木马病毒的前缀是 Trojan，蠕虫病毒的前缀是 Worm，其他前缀还有如 Macro、Backdoor、Script 等。

病毒名是指一个病毒名称，如以前很有名的 CIH 病毒，它和它的一些变种都是统一的 CIH，还有振荡波蠕虫病毒，它的病毒名则是 Sasser。

病毒后缀是指一个病毒的变种特征，一般是采用英文中的 26 个字母来表示的，如 Worm. Sasser. c 是指振荡波蠕虫病毒的变种 c。如果病毒的变种太多了，那也可以采用数字和字母混合的方法来表示病毒的变种。

2. 计算机病毒的分类

计算机病毒按不同的分类标准，可以有许多不同的分类。

(1) 按病毒寄生的媒体。

按寄生的媒体病毒可以划分为网络病毒、文件病毒和引导型病毒。网络病毒通过计

算机网络传播感染网络中的可执行文件；文件病毒感染计算机中的文件（如.COM，.EXE，.DOC 等）；引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。还有这三种情况的混合型，例如多型病毒（文件和引导型）感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

（2）按病毒传染的方法。

按传染的方法病毒可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后，把自身的内存驻留部分放在内存中，这一部分程序挂接系统调用并合并到操作系统中，它处于激活状态，一直到关机或重新启动；非驻留型病毒在得到机会激活时并不感染计算机内存，一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留型病毒。

（3）按病毒破坏的能力。

按破坏的能力病毒可分为无害型、无危险型、危险型、非常危险型。无害型病毒除了传染时减少磁盘的可用空间外，对系统没有其他影响；无危险型病毒仅仅是减少内存、显示图像、发出声音及同类音响；危险型病毒在计算机系统操作中造成严重的错误；非常危险型病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。一些现在的无害型病毒也可能会对新版的 DOS、Windows 和其他操作系统造成破坏。例如，在早期的病毒中，有一个“Denzuk”病毒在 360K 磁盘上不会造成任何破坏，但是在后来的高密度软盘上却能引起大量的数据丢失。

（4）按病毒的算法。

按算法病毒可分为伴随型、蠕虫型、寄生型。

伴随型病毒并不改变文件本身，它们根据算法产生.EXE 文件的伴随体。

蠕虫型病毒不改变文件和信息，利用网络从一台计算机的内存传播到其他计算机内存。

寄生型病毒是除了伴随型和蠕虫型病毒以外的其他病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播，按其算法不同又可分为：

① 练习型病毒，病毒自身包含错误，不能进行很好的传播，例如一些病毒在调试阶段。

② 诡秘型病毒，它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

③ 变型病毒（又称幽灵病毒），这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般的做法是由一段混有无关指令的解码算法和被变化过的病毒体组成。

（5）按病毒的特性。

按病毒的特性可分为系统病毒、蠕虫病毒、木马病毒与脚本病毒等。常见的病毒类型与特性如表 6-1 所示。

表 6-1　常见的病毒类型与特性

病毒类型	病毒前缀	共有特性	典型病毒
系统病毒	Win32、PE、Win95、W32、W95	可以感染 Windows 操作系统的 *.exe 和 *.dll 文件	CIH 病毒
蠕虫病毒	Worm	通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性	冲击波(阻塞网络)、小邮差(发带毒邮件)
木马病毒	Trojan	通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息	QQ 消息尾巴木马 Trojan. QQ3344 网络游戏木马病毒 Trojan. LMir. PSW. 60
黑客病毒	Hack	有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的计算机，而黑客病毒则会通过该木马病毒来进行控制	网络枭雄 Hack. Nether. Client
脚本病毒	Script、VBS、JS	使用脚本语言编写，通过网页进行传播的病毒	红色代码 Script. Redlof 欢乐时光 VBS. Happytime 十四日 Js. Fortnight. c. s
宏病毒	Macro，第二前缀是 Word、Excel	感染 Office 系列文档，然后通过 Office 通用模板进行传播	梅丽莎 Macro. Melissa
后门病毒	Backdoor	通过网络传播，给系统开后门	IRC 后门 Backdoor. IRCBot
病毒种植程序病毒	Dropper	运行时会从体内释放出一个或几个新的病毒到系统目录，由释放出来的病毒进行破坏	冰河播种者 Dropper. BingHe2. 2C MSN 射手 Dropper. Worm. Smibag
破坏性程序病毒	Harm	本身具有好看的图标来诱惑用户点击，当用户点击后，便会产生破坏	格式化 C 盘 Harm. formatC. f 杀手命令 Harm. Command. Killer
捆绑机病毒	Binder	使用特定的程序将病毒与应用程序捆绑起来	捆绑 QQ Binder. QQPass. QQbin 系统杀手 Binder. Killsys

6.1.5　计算机病毒的传播途径

目前计算机病毒有以下传播途径：

(1) 通过计算机硬件。

通过含有固化病毒程序的硬件，计算机会受到病毒入侵。例如海湾战争爆发一年前，美国就派间谍把伊拉克将要进口的一批打印机在法国计算机公司里装上带病毒的芯片，使病毒得以传播。

(2) 通过存储介质。

一些存储介质如光盘、移动硬盘等都是病毒藏身之地。光盘因为容量较大，存储了大

量可执行文件，大量的病毒就有可能藏身在光盘中。以牟利为目的的盗版软件的制作过程中不可能为病毒防护担负专门的责任，也不会有真正可靠可行的技术保障避免病毒的传入、传染、流行和扩散。现在，盗版光盘的泛滥给病毒的传播带来了极大的便利，甚至有些光盘上的杀毒软件本身也带有病毒。另外，由于复制大容量文件的需要，一些移动硬盘和 U 盘也成为现代人们的必备之物，在不断使用中就会担当病毒传播的媒介。

（3）通过网络。

个人计算机的普及和计算机网络的发展使病毒可以更广泛、更迅速地入侵计算机，网络已经成为病毒传播的主要途径。病毒通过网络传播主要有以下几种方式：①通过电子邮件入侵计算机。②通过网站下载入侵计算机。③通过即时通信工具入侵计算机。④通过 BBS 入侵计算机。

计算机病毒传播途径如图 6-2 所示：

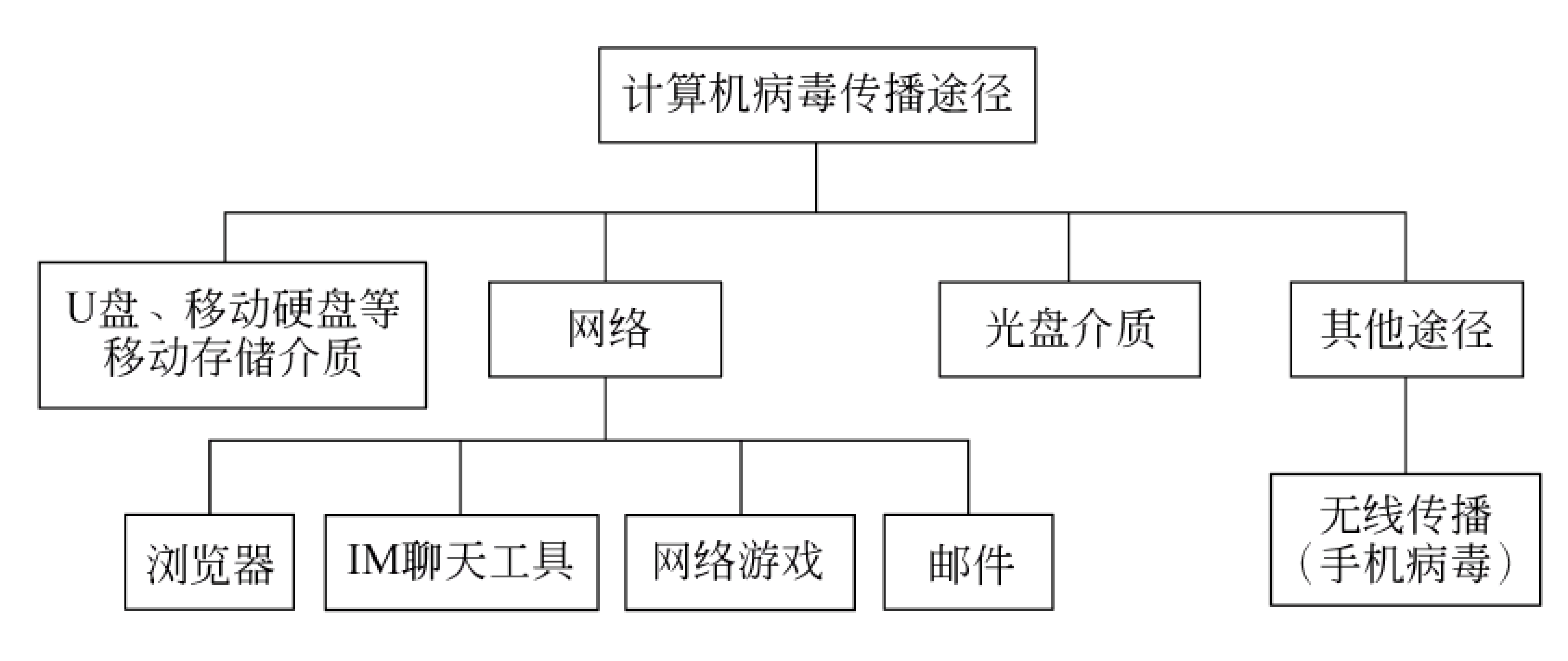


图 6-2　计算机病毒传播途径

从图 6-2 可以看出，凡是在计算机之间可以交换信息的途径，包括移动存储介质、计算机网络等，都是计算机病毒的传播途径。尤其是计算机网络这个途径，虽然出现得较晚，但是危害巨大。

随着网络的延伸，无线局域网和 3G 无线接入等技术的发展，无线电波也将成为计算机病毒的传播途径之一。

6.2　传统的计算机病毒

传统的计算机病毒是指基于 DOS 操作系统而生成的病毒，但随着 Windows 操作系统的普及，有相当一部分病毒又随之寄生在 Windows 操作系统中，本节主要讲述传统的文件型病毒、引导型病毒与宏病毒的特点与防治方法。

6.2.1　DOS 病毒

1. DOS 操作系统

DOS 是磁盘操作系统（disk operating system）的缩写，它是一个单用户、单任务的操作系统，是 IBM PC 机及兼容机曾经使用最广泛的操作系统。DOS 的主要功能是进行文件管理和设备管理。

2. DOS 病毒的特点

DOS 病毒指在计算机病毒发展初期针对 DOS 操作系统开发的病毒。目前几乎没有新制作的 DOS 病毒，由于 Windows 9X 病毒的出现，DOS 病毒几乎绝迹。但 DOS 病毒在 Win 9X 环境中仍可以发生感染，因此若执行染毒文件，Win 9X 用户也会被感染。有相当一部分 DOS 病毒可在 Windows 的 DOS 窗口下运行并传播。

目前发现的所有病毒中有一半以上都是 DOS 病毒。大部分 DOS 病毒都是制造者通过对公开代码进行一定变形而制作的恶作剧，这些病毒绝大部分是感染 DOS 可执行文件，如：.EXE 文件，.COM 文件，或者是.BAT 文件等。此外，大部分 DOS 病毒都有一个共同的特性，即通常在特定条件下发作，破坏性比较严重的病毒会破坏硬盘中的重要资料，甚至重新格式化硬盘。

早期常见的以日期为触发条件的病毒发作现象如表 6-2 所示。

表 6-2　常见的以日期为触发条件的病毒

病 毒 名 称	发病的特定条件	发 病 情 形
Michelangelo(米开朗琪罗)	每年 3 月 6 日	格式化硬盘
Jerusalem(耶路撒冷)	每逢 13 号的星期五	破坏执行程序
Casino(赌场)	每逢 1 月 15 日，4 月 15 日，8 月 15 日	出现“我是赌场病毒，来吧，我们赌一把”的信息
Flip(翻转)	每月 2 号	屏幕翻转
Sunday(星期天)	每逢星期日	计算机无法使用
Fish(鱼)	每月 1 日，11 日，21 日，31 日	屏幕右上方出现信息
Taiwan NO.1(台湾一号)	每月 13 号	出现心算画面
猜拳病毒	每月的 1 日，6 日，15 日，25 日	出现猜拳画面
剧场病毒	每月 1 日和 15 日	出现一哭一笑面具图案
钓鱼台	每月 5 日和 20 日	出现“钓鱼台岛是中国领土……”等对话窗口
BOZA	每月 31 日	出现“成名的滋味，越来越过瘾……”等信息

6.2.2　文件型病毒

1. 文件型病毒概述

文件型病毒是通过操作系统的文件系统进行感染的病毒，它对计算机的源文件进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播的目的。

文件型病毒可以感染所有标准的 DOS 可执行文件：包括批处理文件、DOS 下的可加载驱动程序(.SYS)文件以及普通的 COM/EXE 可执行文件。还可以感染所有 Windows

操作系统可执行文件，包括：Windows 3.X 版本，Windows 9.X 版本，Windows NT 和 Windows 2000 版本下的可执行文件，后缀名是.EXE、.DLL 或者.VXD、.SYS。

2. 文件型病毒的清除

(1) 文件型病毒都驻留内存，在正常模式下，由于带毒文件正在运行，所以清除文件型病毒最好在 DOS 模式下操作。

(2) 许多文件型病毒也会通过网络感染，所以杀毒时一定要断掉网络连接，特别在局域网中，一定要把所有计算机上的病毒全都查杀干净以后才可以联网。如果你面对的是一个中大型的局域网，可以考虑购买企业版(网络版)的杀毒软件进行管理。

(3) 由于文件型病毒都是要对宿主文件(也就是要被感染的文件)进行修改，把自身代码添加到宿主文件上，所以会造成一些结构比较复杂的文件损坏，例如一些自解压缩文件(通常是一些软件的安装文件)、带有自校验功能的文件无法运行，当它感染了系统文件，还会造成系统问题(例如经常出现“非法操作”等)，出现这些症状则文件是无法修复的。

6.2.3 引导型病毒

1. 引导型病毒的特点

引导型病毒指寄生在磁盘引导区或主引导区的计算机病毒。它利用系统引导时不对主引导区的内容正确与否进行判别的缺点，侵入系统，驻留在内存，监视系统运行，伺机传染和破坏。

引导型病毒有以下特点：

(1) 引导型病毒是在安装操作系统之前进入内存，寄生对象又相对固定，因此该类型病毒基本上不得不采用减少操作系统所掌管的内存容量的方法来驻留内存高端。而正常的系统引导过程一般是不减少系统内存的。

(2) 引导型病毒需要把病毒传染给软盘，一般是通过修改 INT 13H 的中断向量，而新 INT 13H 中断向量段址必定指向内存高端的病毒程序。

(3) 引导型病毒感染硬盘时，必定驻留硬盘的主引导扇区或引导扇区，并且只驻留一次，因此引导型病毒一般都是在软盘启动过程中把病毒传染给硬盘的，而正常的引导过程一般是不对硬盘主引导区或引导区进行写盘操作的。

(4) 引导型病毒的寄生对象相对固定，把当前的系统主引导扇区和引导扇区与干净的主引导扇区和引导扇区进行比较，如果内容不一致，可认定系统引导区异常。

2. 清除与防范引导区病毒

(1) 清除引导区病毒。

如果用干净的启动盘启动计算机以后发现不能访问硬盘，而且硬盘不是 NTFS 格式，但是用硬盘启动计算机以后可以访问硬盘，则说明你的计算机感染了加密的引导区病毒。遇到这种病毒时，应该让系统自己引导计算机，让病毒自己解密，然后用杀毒软件备

份引导区的信息(目前国产的三大杀毒软件都有此功能),然后再用干净的启动盘启动计算机,把刚刚备份出来的引导区信息再写回硬盘就可以了。

(2) 防范引导区病毒。

引导区病毒只有用染有病毒的软盘或光盘启动计算机的时候才会感染,所以养成良好的习惯是防范这种病毒的关键,对不明来路的软盘使用前要先查毒;不用计算机的时候不要把软盘、光盘留在驱动器里(许多计算机感染这个病毒都是由于用了带有病毒的可引导光盘启动计算机所造成的);另外,最好在主板的设置里把防病毒一项打开。

6.2.4　宏病毒

1. 录制"宏"

所谓宏(Macro)就是把一系列的指令组织成一独立的命令,在操作时可以直接利用事先编好的宏自动运行相应命令完成某项特定的任务。Office 中的 Word 和 Eecel 都有宏,下面介绍如何使用 Word 中的宏来画填空题的空格线。

画空格线时需要先切换到英文输入状态,再按住"Shift+_"键来画,在操作中必须不断地切换输入法,而 Word 2007 中提供的宏,能用一快捷键来代替这种复杂的操作。

录制宏的步骤如下:

(1) 在 Word 2007 中单击"视图"标签,选择"宏"选项中的"录制宏"命令,打开如图 6-3 所示的"录制宏"对话框,在"宏名"文本框中输入宏名,如 "line"。

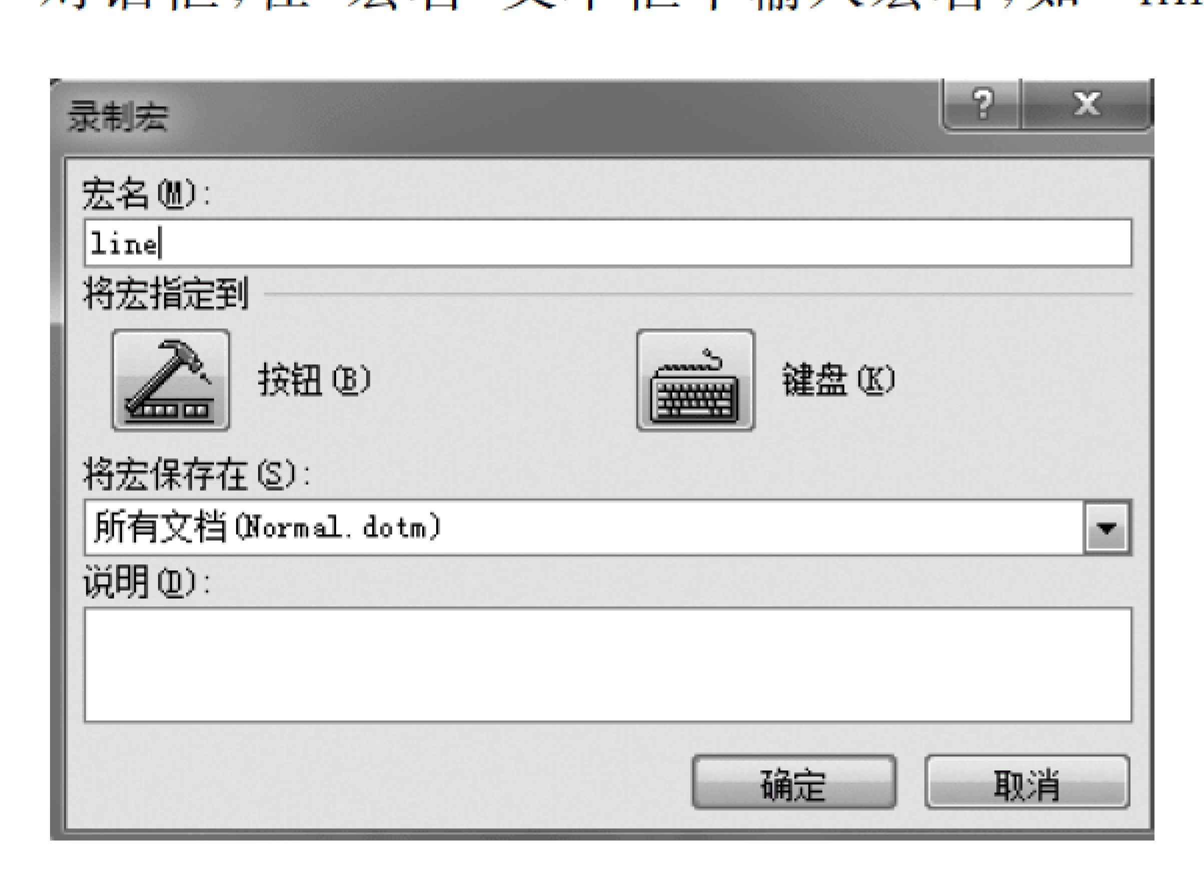


图 6-3　"录制宏"对话框

(2) 单击"键盘"图标,打开如图 6-4 所示的"自定义键盘"对话框,在键盘上按下用来代替该宏操作的快捷键,如 Ctrl+K,然后单击【指定】按钮,并在"将更改保存在"下拉对话框中选择使用宏的文档名,最后单击【关闭】按钮。

(3) 单击【关闭】按钮后,进入录制状态,这时按住"Shift+_"键画一段空格线,然后,选择"宏"选项中的"停止录制"命令,就完成了宏的录制,以后在编辑过程中只要按下 Ctrl+K 组合键就完成了空格线的输入。

2. 宏病毒的定义

宏病毒是利用系统内置宏命令编写的一个或多个具有病毒特点的宏的集合,用来感

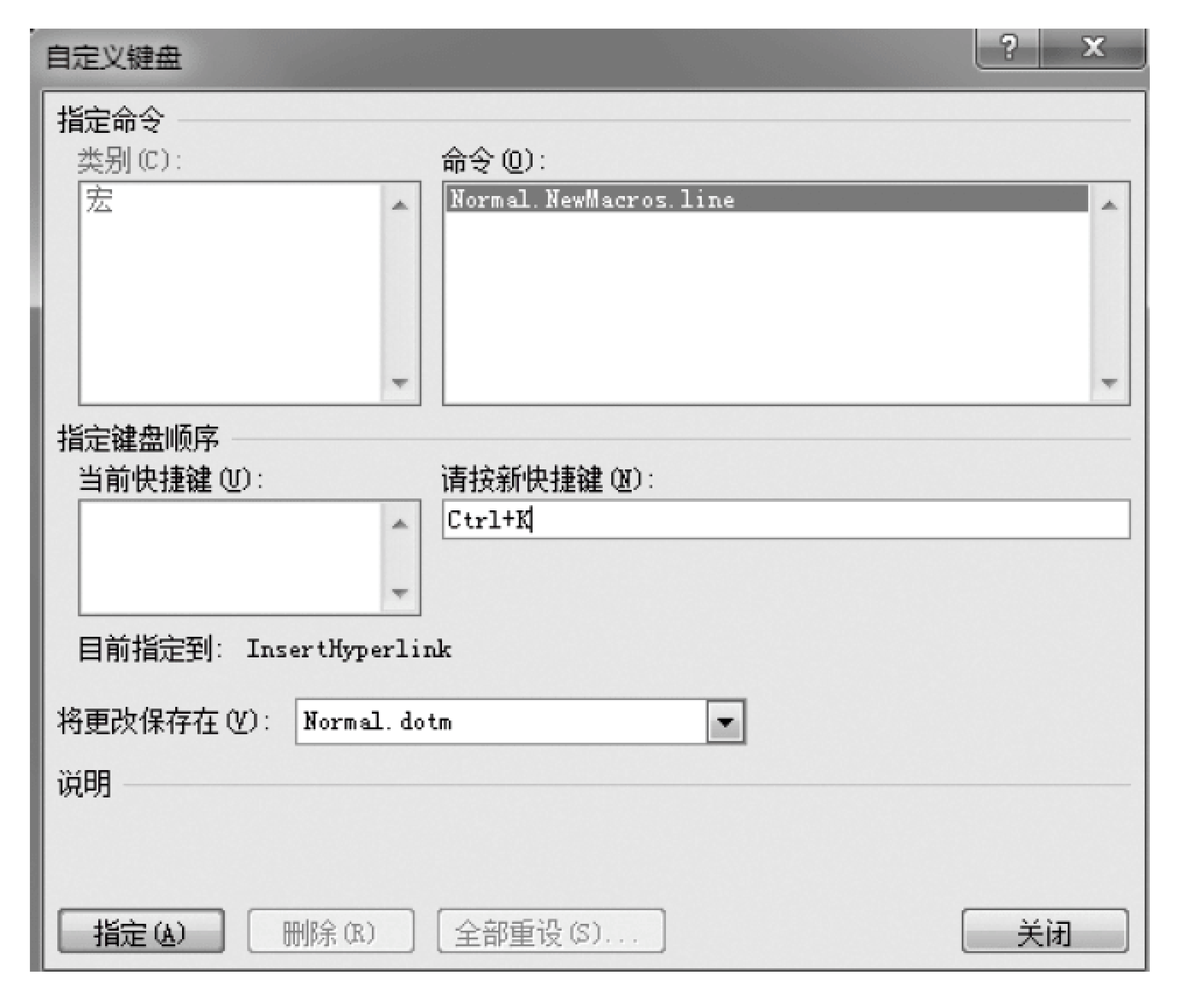


图 6-4 “自定义键盘”对话框

染 Word、Excel 文件和模板文件，Word、Excel 内置的宏编程语言使得宏病毒有机可乘，可以把病毒宏命令代码附加在指定文件上，通过文件的打开、关闭或某项功能被调用时来获取控制权，实施病毒所定义的非法操作。

3. 宏病毒的激活与感染

当打开或建立 Word 文档时，系统都会自动装入 Normal.dot(通用模板)并执行其中的宏。Word 打开文件时，首先检查文件内是否包含自动执行的宏，若有 AutoOpen 宏，Word 就启动它。若有 AutoClose 宏，则系统在关闭一个文件时会自动执行它。

宏病毒至少会包含一个以上的自动宏，当 Word 运行这类自动宏时，实际上就是在运行病毒代码；当病毒代码被执行过后，它就会将自身复制到通用宏集合内。当 Word 系统退出时，它会把病毒宏自动地保存到模板文件 Normal.dot 中。这样，只要一启动 Word，就会自动运行 Normal.dot 文件，宏病毒就会被激活，所有创建或打开的文档都会感染上这种宏病毒。感染上宏病毒的文档，会随着在其他计算机上的打开而感染其他计算机。

4. 宏病毒的特点

(1) 传播极快。Word 宏病毒通过.doc 文档及.dot 模板进行自我复制及传播，而计算机文档是交流最广的文件类型。特别是 Internet 的普及和 E-mail 的大量应用更为 Word 宏病毒传播拓展了道路。

(2) 制作变种方便。Word 使用宏语言来编写宏指令。目前，世界上的宏病毒原型已有几十种，其变种与日俱增，究其原因还是 Word 的开放性所致。

(3) 破坏可能性极大。鉴于宏病毒用 VBA(早期使用 Word Basic)语言编写，VBA 或 Word Basic 语言提供了许多系统级底层调用。如直接使用 DOS 系统命令调用 Windows VBA、API、DDE、DLL 等。这些操作均可能对系统直接构成威胁，而 Word 在指令安全性、完整性上的检测能力很弱，破坏系统的指令很容易被执行。

(4) 宏病毒的兼容性不高。Word 模板(template)是开发 Word 应用程序的唯一方法,宏病毒也不例外。宏病毒在 doc 文档、dot 模板是以 BFF(binary file format)格式存放的,这是一种加密压缩格式,不同的 Word 版本,格式可能不兼容。

5. 宏病毒的症状

宏病毒的检测非常容易,只要留意一下常用的 Office 系统软件是不是出现了一些不正常的现象,就可以知道计算机是不是染上了宏病毒。

(1) 通用模板中出现宏。

大多数宏病毒是通过感染通用模板 Normal. dot 进行传播的。当使用“宏”菜单命令时,在通用模板上发现有 AutoOpen 等自动宏、FileSave 等标准宏或一些怪名字的宏,而用户又没有使用特殊的宏的时候,用户文档很可能是染上了宏病毒,因为大多数用户的通用模板是没有宏的。

(2) 无故出现存盘操作。

打开一个 Word 文档后,没有经过任何改动,立刻就有存盘操作。

(3) Word 功能混乱,无法使用。

一些病毒能够破坏 Word 的运行机制,使文档的打开、关闭、存盘等操作无法正常进行。最常见的是原 Word 文档无法另存为其他格式文件。如 Word 的. doc 文档文件感染病毒后,属性已发生了变化,只能以模板文件方式存盘。

(4) Word 菜单命令消失。

一些病毒感染系统时,出于隐形或自我保护目的,会关闭 Word 菜单的某些命令。

(5) Word 文档的内容发生变化。

Word 文档中加入陌生的信息。

6. 宏病毒的预防与清除

根据宏病毒产生的机理,可采用以下措施预防和消除宏病毒。

(1) 将 Word 文档保存成为 rtf 或 txt 格式。因为宏病毒的存在依赖于系统对宏的支持,而 rtf 或 txt 格式都不支持宏的功能。

(2) 在 AutoExec. bat 文件中加入命令:Winword. exe/mDisableAutoMacros。宏病毒是通过自动执行宏的方式来激活的,此命令用来终止自动宏的执行。

(3) 激活 Word 本身的宏病毒防护功能。将安全级设定为“高”。

(4) 删除 Normal. dot 中名称为 AutoOpen、AutoClose、AutoExit、FileSave、FileSaveAs 和 FileExit 等宏。保持 Word 系统的清洁。

(5) 给 Normal. dot 模板加设密码保护。没有正确的密码,宏病毒当然无法修改 Normal. dot,也就无处藏身了。

(6) 备份干净的 Normal. dot 模板文件。在遇到有宏病毒的时候,用备份的 Normal. dot 替换位于“MSoffice\Template”目录下的通用模板 Normal. dot 文件。

(7) 使用专业的杀毒软件。

6.3 互联网下的典型病毒

随着互联网的普及,以及 Windows 操作系统被广大用户所使用,传播的主要病毒类型也发生了迁移。

本节着重介绍互联网与 Windows 操作系统下的蠕虫病毒、特洛伊木马、脚本病毒、手机病毒及其他操作系统病毒的特点及其防治方法。

6.3.1 互联网的瘟疫——蠕虫病毒

1. 蠕虫病毒的特点

(1) 蠕虫病毒是无需计算机使用者干预即可运行的独立程序,它通过不停地获得网络中存在漏洞的计算机上的部分或全部控制权来进行传播。

(2) 蠕虫病毒具有传统计算机病毒的一些共性,同时具有自己的特征,如不利用文件寄生(有的只存在于内存中),对网络造成拒绝服务,以及可以和黑客技术相结合等。

(3) 蠕虫病毒破坏性极大,网络的发展使得蠕虫可以在短短的时间内蔓延整个网络,造成网络瘫痪。

(4) 蠕虫病毒很难根除。

2. 蠕虫病毒的传播过程

在假设系统已经感染蠕虫病毒,并且蠕虫病毒处于运行状态的前提条件下可以将蠕虫病毒传播的过程简化为 4 个主要的步骤:

(1) 目标获取:为了实现病毒的传播,蠕虫病毒必须设法找到下一个攻击的目标主机,目标主机可以通过以下方法获得:①IP 地址扫描;②E-mail 地址列表;③网络文件系统传输。

(2) 传送病毒代码:一旦找到目标主机,蠕虫病毒就开始设法传送病毒代码到目标主机,传送病毒代码的方式主要有以下几种:①网络文件系统;②电子邮件;③Web 客户端;④远程命令执行;⑤利用缓冲区溢出等程序错误。

(3) 执行病毒代码:仅仅把病毒代码传送到目标主机还是远远不够的,还必须要使用某种机制来触发病毒代码的执行,通常蠕虫病毒会采用以下方法来执行病毒代码:①直接从命令行执行;②缓冲区溢出或者其他程序攻击;③E-mail 客户端;④Web 客户端;⑤用户干预;⑥目标主机自动执行。

(4) 附加代码传送:有的蠕虫病毒在第三步传送病毒代码的时候不是一次完成,仅仅传送蠕虫病毒的部分代码,在获得目标主机的控制权之后,再完成后继代码的传送,一般通过 FTP 或 TFTP 和网络文件系统来完成。

3. 蠕虫病毒的清除方法

(1) 用杀毒软件查杀。每次网络蠕虫爆发后,杀毒软件公司都会根据病毒的特征及

时制作相应的杀毒软件,所以用户要经常了解最新的蠕虫病毒及相应的杀毒软件,并及时安装查杀。另一方面,由于蠕虫病毒会迅速变种,用户还要及时升级杀毒软件。

(2) 手工清除。可以根据蠕虫病毒的工作机理手工清除蠕虫病毒。

手工清除冲击波病毒的步骤:

① 先拔掉网线,启动任务管理器,在其中查找 msblast.exe 进程,找到后在进程上单击右键,选择"结束进程"。

② 用文件搜索的方法查找到 msblast.exe,然后删除该文件。

③ 修改注册表,单击"开始"→"运行"菜单,在"打开"文本框中输入 regedit 命令,然后单击【确定】按钮,打开"注册表编辑器"对话框,从中找到"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"后,在右边找到键值"windows auto update=msblast.exe",将其删除。

④ 重启计算机并打上补丁,以免计算机再一次遭受蠕虫的攻击。

⑤ 连接网线,恢复正常工作。

4. 蠕虫病毒的预防

(1) 为系统打上补丁包,堵住系统漏洞。目前大部分网络蠕虫都是利用计算机系统漏洞来攻击计算机的,并且从公布计算机系统漏洞到相应的蠕虫病毒问世的时间间隔越来越短,所以及时了解发现系统存在的漏洞并下载相应的补丁进行修补是非常关键的防御蠕虫病毒的重要措施。

(2) 采用入侵检测技术。入侵检测是一种主动防御网络攻击的技术,可以与防火墙联动,起到网络蠕虫预警的作用。

(3) 接种疫苗技术。接种疫苗技术是当网络蠕虫爆发时网管人员采取的一种主动防御技术。根据网络蠕虫不同的攻击特性设计出相应的疫苗,然后对易感主机进行疫苗接种,使接种后的计算机对相应的网络蠕虫有免疫功能,从而避免了网络蠕虫的攻击。

(4) 卸载 WSH 功能。由于部分蠕虫病毒是采用 VBScript 脚本语言编写的,而 VBScript 代码必须由 WSH(windows script host)解释执行。在不影响计算机的正常工作的前提下,可以将 WSH 功能卸载,使蠕虫病毒失去运行的环境。

6.3.2 隐藏的危机——特洛伊木马

1. 特洛伊木马简介

特洛伊木马是一个程序,它驻留在目标计算机中。在目标计算机启动时,它自动启动,然后在某一端口进行侦听。如果在该端口收到数据,则对这些数据进行识别,然后在目标计算机上进行一些操作,例如窃取口令、复制或删除文件,或者重新启动计算机。作为木马,一定符合下面三个条件:①需要一种启动方式,一般在注册表启动组中;②需要在内存中运行才能发挥作用;③占用一个端口。

完整的木马程序一般由两个部分组成:一个是服务端(被控制端),另一个是客户端(控制端)。攻击者通常利用绑定程序工具将服务器部分绑定到某个合法软件上,诱使用

户运行合法软件。只要用户一运行软件，特洛伊木马的服务部分就在用户毫无知觉的情况下完成安装。

2. 特洛伊木马的伪装

木马的伪装方式主要有以下三种：

（1）集成在程序中。木马制作者为了不让用户轻易地把木马程序删除，就用技术手段把木马集成到应用程序里；

（2）伪装在普通文件中。木马制作者把木马程序伪装成图片或文本，用户点击带有木马的图片或文本时，木马便安装到了用户的计算机中；

（3）伪装在超链接中。木马传播者在网页上放置木马引诱用户点击，点击后用户计算机便被安装木马。

3. 特洛伊木马的启动

如果特洛伊木马加入到用户经常执行的程序（例如 explorer. exe）中，用户执行该程序时，木马就会自动启动。木马有以下几种启动方式：

（1）在 Win. ini 中启动。

在 Win. ini 的[windows]字段中有启动命令“load＝”和“run＝”，在一般情况下“＝”后面是空白的，如果有如下命令：

```
run==C:\windows\file.exe
load=C:\windows\file.exe
```

这个 file. exe 很可能就是木马了。

（2）在 System. ini 中启动。

System. ini 位于 Windows 的安装目录下，其[boot]字段的 shell＝Explorer. exe 是木马喜欢隐藏加载之所，木马通常的做法是将字段变为“shell＝explorer. exe 程序名”，则后面跟着的那个程序就是“木马”程序，要在硬盘中找到这个程序并将其删除。这类病毒很多，例如“尼姆达”病毒就会把该项修改为“shell＝explorer. exe load. exe—dontrunold”。

另外，在 System. ini 中的[386Enh]字段，要注意检查在此字段内的“driver＝路径\程序名”，这里有可能被木马所利用。再有，在 System. ini 中的[mic]、[drivers]、[drivers32]这 3 个字段，这些字段也是起到加载驱动程序的作用，但也是增添木马程序的场所。

（3）利用注册表加载启动。

如下所示注册表位置都是木马喜欢藏身之所，要注意检查一下，有什么程序在其下。

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrenVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

（4）在 Autoexec. bat 和 Config. sys 中加载启动。

在 C 盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都需要控制

端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件才行，而且采用这种方式不是很隐蔽。容易被发现，所以在 Autoexec. bat 和 Config. sys 中加载木马程序的并不多见，但也不能因此而掉以轻心。

(5) 在 Winstart. bat 中启动。

Winstart. bat 是一个特殊性不亚于 Autoexec. bat 的批处理文件，也是一个能自动被 Windows 加载运行的文件。它多数情况下为应用程序及 Windows 自动生成，在执行了 Win. com 并加载了多数驱动程序之后开始执行(这一点可通过启动时按 F8 键再选择逐步跟踪启动过程的启动方式得知)。由于 Autoexec. bat 的功能可以由 Winstart. bat 代替完成，因此木马完全可以像在 Autoexec. bat 中那样被加载运行，危险由此而来。

(6) 在启动组中启动。

木马隐藏在启动组虽然不是十分隐蔽，但这里的确是自动加载运行的好场所，因此还是有木马喜欢在这里驻留的，因此，要注意经常检查启动组。

启动组对应的文件夹为 C：\Windows\start menu\programs\startup，在注册表中的位置为：HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Explorer\shell Folders Startu＝“c：\windows\start menu\programs\startup”。

(7) 在 *. ini 中启动。

*. ini(Winint. ini)是应用程序的启动配置文件，利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖这同名文件，就可以达到启动木马的目的。

(8) 修改文件关联。

修改文件关联是木马们的常用手段(主要是国产木马，国外的木马大都没有这个功能)，在正常情况下 TXT 文件的打开方式为 Notepad. exe 文件，但一旦中了文件关联木马，txt 文件打开方式就会被修改为用木马程序打开，如著名的国产木马冰河就是这样干的。“冰河”就是通过修改 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的键值，将“C：\WINDOWS\NOTEPAD. EXE”改为“C：\WINDOWS\SYSTEM\SYSEXPLR. EXEl”，这样，一旦双击一个 TXT 文件，原本应用 Notepad 打开该文件，现在却变成启动木马程序了。需要注意，不仅仅是 TXT 文件，其他诸如 HTM、EXE、ZIP、COM 等都是木马的目标。对付这类木马，只能经常检查 HKEY_C\shell\open\command 主键，查看其键值是否正常。

(9) 绑定文件。

实现这种触发条件首先要控制端和服务端已通过木马建立连接，然后用工具软件将木马文件和某一应用程序捆绑在一起，再上传到服务端覆盖源文件，这样即使木马被删除了，只要运行绑定了木马的应用程序，木马又会安装上去，绑定到某一应用程序中。如绑定到系统文件，那么每一次 Windows 启动均会启动木马。

(10) 反弹端口型木马的主动连接方式。

反弹端口型木马由于它与一般的木马相反，其服务端(被控制端)主动与客户端(控制端)建立连接，并且监听端口一般开在 80，所以如果没有合适的工具、丰富的经验真的很难防范。

4. 特洛伊木马的检测

检测木马的存在，可以通过查看 System.ini 文件的[boot]目录、查看 Win.ini 文件、查看启动组、查看注册表等，看有否可疑文件或内容存在。另外，还可以通过在“运行”窗口中输入 netstat-a 命令来查看有否不明端口处于监听状态，如果目前没有任何网络服务操作，那么监听该端口的就是特洛伊木马了。

5. 特洛伊木马的清除

删除木马时，首先要将网络断开，再用相应的方法来删除它。

(1) 通过木马的客户端程序删除。

在 Win.ini 或 system.ini 的文件中找到可疑文件判断木马的名字和版本，然后在网络上找到相应的客户端程序，下载并运行该程序，在客户程序对应位置填入本地计算机地址：127.0.0.1 和端口号，就可以与木马程序建立连接，再由客户端的删除木马服务器的功能来删除木马。

(2) 手工删除。

在“命令提示符”窗口中用 Msconfig 打开系统配置实用程序，可对 Win.ini、system.ini 和启动项目进行编辑。屏蔽掉非法启动项。

在“命令提示符”窗口中用 rededit 打开注册表编辑器，对注册表进行编辑。先由上面的方法找到木马的程序名，再在整个注册表中搜索，并删除所有木马项目。由查找到木马程序注册项，分析木马文件在硬盘中的位置，然后再进行删除。重新启动以后再用上面各种检测木马的方法对系统进行检查，以确保木马确实被删除。

(3) 工具删除。

上面两种方法对于非专业人员来说操作起来并不容易，但现在已有许多非常好的木马专杀工具，大家可以根据自己需要下载或购买使用。利用工具删除，可以免除烦琐的操作，完全由软件程序自行完成。

6.3.3 网上冲浪的暗流——脚本病毒

1. 脚本病毒简介

脚本程序的执行离不开 WSH(windows script host)。WSH 是微软提供的一种基于 32 位 Windows 平台的、与语言无关的脚本解释机制。它使得脚本能够直接在 Windows 桌面或命令提示符下运行。WSH 可以使用 VBS、JavaScript 编写脚本文件。利用 WSH，用户能够操纵 WSH 对象、ActiveX 对象、注册表和文件系统，还可访问活动目录服务。WSH 脚本程序很简单，大部分高级语言具有的功能，它基本上都具备，所以许多病毒也利用了这一点，通过 WSH 来编制病毒程序。

浏览器依赖于 WSH 提供的 VBS、JavaScript 脚本引擎，解释网页中嵌入的脚本代码。当一个含有以 VBS、JavaScript 编制的脚本的网页下载到一个兼容的浏览器中时，浏览器将自动执行其脚本。

2. 脚本病毒的特点

(1) 编写简单。一个以前对病毒一无所知的病毒爱好者可以在很短的时间里编出一个新型病毒来。

(2) 破坏力大。其破坏力不仅表现在对用户系统文件及性能的破坏,还可以使邮件服务器崩溃,网络发生严重阻塞。

(3) 感染力强。由于脚本是直接解释执行,并且它不需要像 PE 病毒那样,需要做复杂的 PE 文件格式处理,因此这类病毒可以直接通过自我复制的方式感染其他同类文件,并且自我的异常处理变得非常容易。

(4) 传播范围大。这类病毒通过 htm 文档,E-mail 附件或其他方式,可以在很短的时间内传遍世界各地。

(5) 病毒源码容易被获取变种多。由于 VBS 病毒解释执行,其源代码可读性非常强,即使病毒源码经过加密处理后,其源代码的获取还是比较简单。因此,这类病毒变种比较多,稍微改变一下病毒的结构,或者修改一下特征值,很多杀毒软件可能就无能为力。

(6) 欺骗性强。脚本病毒为了得到运行机会,往往会采用各种让用户不太注意的手段,譬如,邮件的附件名采用双后缀,如.jpg、.vbs,由于系统默认不显示后缀,这样,用户看到这个文件的时候,就会认为它是一个 jpg 图片文件。

(7) 病毒生产机实现起来非常容易。所谓病毒生产机,就是可以按照用户的意愿,生产病毒的机器(当然,这里指的是程序),目前的病毒生产机,之所以大多数都为脚本病毒生产机,其中最重要的一点还是因为脚本是解释执行的,实现起来非常容易。

3. 脚本病毒的危害

网页中嵌入的恶意脚本代码极大地威胁着网络系统安全。它们的危害包括:

(1) 消耗系统资源。通过不断消耗本机系统资源,使计算机不能处理其他进程,导致系统与网络瘫痪。这类病毒大都是利用脚本产生一个死循环,它可以在恶意的网站中出现,也可以被当作邮件的附件发给用户。当用户打开附件时,屏幕出现无数个浏览器窗口,最后不得不关机重新启动。

(2) 非法向用户的硬盘写入文件。已经有部分个人主页或邮件含有可以格式化本地硬盘的恶意代码。

(3) IE 泄密。利用浏览器的漏洞,网页可以读取客户机的文件,或者获取用户账号与密码。

(4) 利用邮件非法安装木马。

4. 脚本病毒的启动

脚本病毒几种典型的获得控制权的方法如下:

(1) 修改注册表项。

Windows 在启动的时候,会自动加载 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\run 下的各键值所指向的程序。脚本病毒可以在此

项下加入一个键值指向病毒程序，这样就可以保证每次计算机启动的时候拿到控制权。VBS修改注册表的方法比较简单，直接调用 wsh. regwrite(strname,anyvalue[,strtype]) 语句即可。

(2) 通过映射文件执行。

譬如，"新欢乐时光"病毒将 dll 的执行方式修改为 wscript. exe。甚至可以将 exe 文件的映射指向病毒代码。

(3) 让用户自己执行。

这种方式其实和用户的心理有关，病毒在发送附件时，采用双后缀的文件名，由于默认情况下，后缀并不显示，例如，文件名为 beauty. jpg. vbs 的 VBS 程序显示为 beauty. jpg，这时用户往往会把它当成一张图片去点击。同样，对于用户自己磁盘中的文件，病毒在感染它们的时候，将原有文件的文件名作为前缀，VBS 作为后缀产生一个病毒文件，并删除原来文件，这样，用户就有可能将这个 VBS 文件看作自己原来的文件运行。

(4) desktop. ini 和 folder. htt 互相配合。

这两个文件可以用来配置活动桌面，也可以用来自定义文件夹。如果用户的目录中含有这两个文件，当用户进入该目录时，就会触发 folder. htt 中的病毒代码。这是"新欢乐时光"病毒采用的一种比较有效的获取控制权的方法，并且利用 folder. htt，还可能触发 exe 文件，这也是病毒得到控制权的一种有效方法。

5. 脚本病毒的预防

VBS 脚本病毒由于其编写语言为脚本，具有如下弱点：①绝大部分 VBS 脚本病毒运行的时候需要用到一个对象 FileSystemObject；②VBScript 代码是通过 WSH 来解释执行的；③VBS 脚本病毒的运行需要其关联程序 wscript. exe 的支持；④通过网页传播的病毒需要 ActiveX 的支持；⑤通过 E-mail 传播的病毒需要 OE 自动发送邮件的功能支持。

针对以上提到的 VBS 脚本病毒的弱点，可以采取如下防范措施：

(1) 禁用文件系统对象 FileSystemObject。用 regsvr32 scrrun. dll /u 这条命令就可以禁止文件系统对象(regsvr32 是 Windows\System 下的可执行文件)，或者直接查找 scrrun. dll 文件删除或者改名。或者在注册表中 HKEY_CLASSES_ROOT\CLSID\下找到一个主键{0D43FE01-F093-11CF-8940-00A0C9054228}的项，直接删除。

(2) 设置 Internet 安全属性。重要的是自定义安全级别，打开 IE 浏览器，单击"Internet 选项"菜单，在安全设置对话框中选择"自定义安全级别"，如图 6-5 所示。把"ActiveX 控件及插件"的一切设置设为禁用，如图 6-6 所示。设置完成后单击【确定】按钮。

(3) 在 Windows 目录中，找到 wscript. exe.，更改名称或者删除，如果觉得以后有机会用到，最好更改名称。

(4) 禁止 OE 的自动收发邮件功能。

(5) 由于蠕虫病毒大多利用文件扩展名做文章，所以要防范它就不要隐藏系统中已知文件类型的扩展名。Windows 默认的是"隐藏已知文件类型的扩展名称"，将其修改为显示所有文件类型的扩展名称。




图 6-5　Internet 属性设置界面

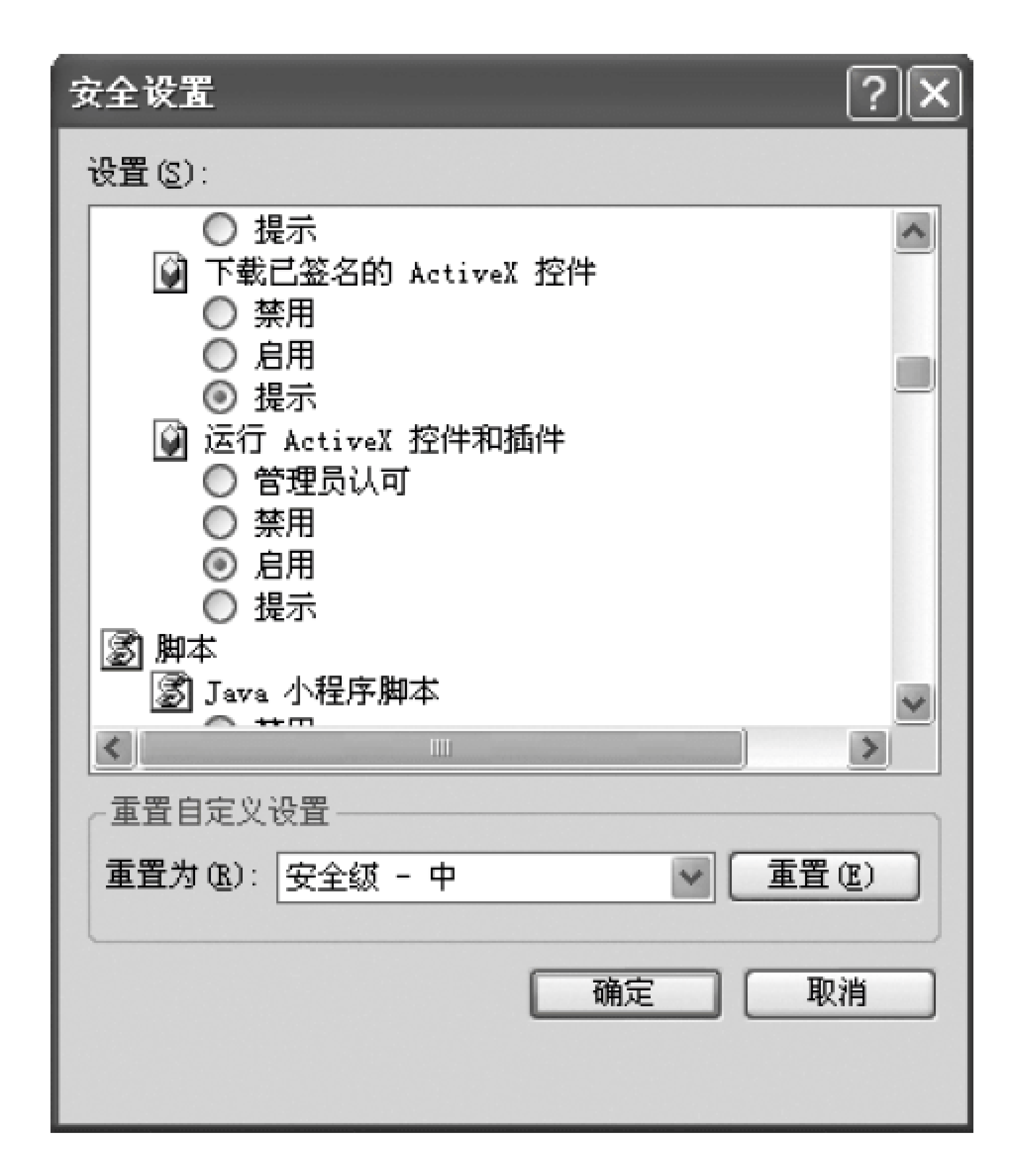


图 6-6　安全设置-Internet 区域设置界面

(6) 将系统的网络连接的安全级别设置至少为“中”，它可以在一定程度上预防某些有害的 Java 程序或者某些 ActiveX 组件对计算机的侵害。

(7) 利用杀毒软件进行清除。

6.3.4　公开的秘密——手机病毒

1. 手机病毒简介

手机病毒是一种具有传染性、破坏性的手机程序。它以手机等移动通信设备为感染对象，以移动运营商网络为平台，通过发送短信、彩信、电子邮件、浏览网站、下载铃声等方式进行传播，从而导致用户手机关机、死机、SIM 卡或芯片损毁、存储资料被删或向外泄露、发送垃圾邮件、拨打未知电话、通话被窃听、订购高额 SP(服务提供者)业务等损失。

最早的手机病毒出现于 2000 年 3 月的西班牙，被命名为“Timofonica”，它可以通过西班牙电信公司的移动系统向系统内的用户发送脏话等垃圾短信，然而“Timofonica”并不属于真正意义上的手机病毒。直到 2004 年 6 月“Cabir”蠕虫病毒出现，这种病毒可以通过诺基亚 s60 系列手机复制，然后不断寻找安装了蓝牙的手机，因为持续的搜索蓝牙设备，从而造成待机能力明显降低并且手机被感染后蓝牙将不受控制。此后，手机病毒开始泛滥。

2. 手机病毒的工作原理

智能手机平台一般都采用嵌入式操作系统(固化在芯片中，常见有诺基亚 Symbian 系统、苹果 iOS 系统和谷歌 Android 系统，一般由 C++、Java 等语言编写)，与 PC 平台的硬件组成类似，所以容易被病毒所攻击。病毒可以通过网络浏览、彩信和电子邮件等途径通过手机的漏洞来侵入手机。

手机病毒传播主要分为三种：

(1) 通过手机外部接口进行传播，例如 USB、蓝牙、红外等。

(2) 通过互联网接入进行传播，例如网站浏览、程序下载等。

(3) 通过手机业务进行传播，例如短信、彩信中的未知链接等。

从后两种传播方式可以看出，手机病毒传播的必要条件是移动运营商要提供数据传输功能，而且手机需要支持 Java 等高级程序写入功能。现在许多具备上网及下载等功能的手机都可能会被手机病毒入侵。图 6-7 展示了现今手机病毒的主要传播途径。

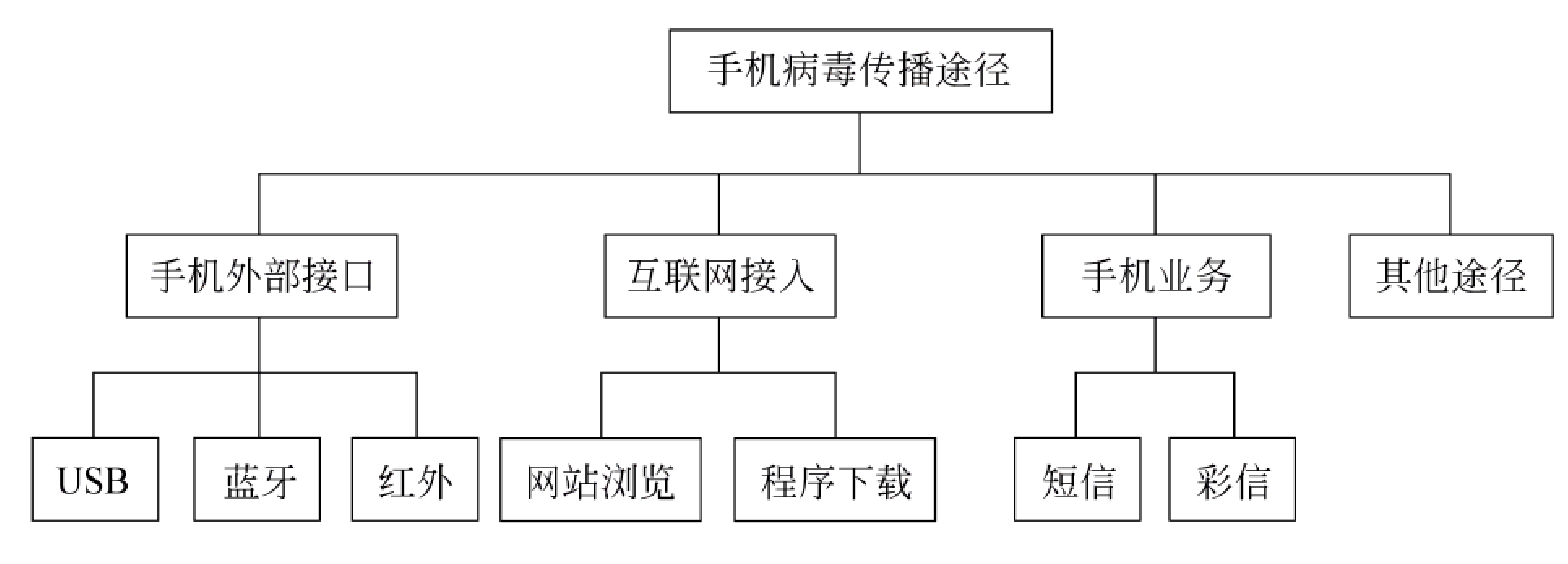


图 6-7 手机病毒传播途径

3. 手机病毒的危害

手机病毒的攻击对象包括两类：手机终端和移动通信网络。

(1) 对手机终端的危害。

手机终端是手机病毒的主要攻击目标，对手机终端的攻击可能会造成手机用户经济、信誉、设备和信息的损害或丧失，其危害形式主要表现为：

① 监听或窃取用户信息。手机木马可以将被感染用户手机中的个人信息、通讯录、图片和文件等传送到指定的地方，导致用户敏感信息的泄露。例如国外已发生过多起公众人物手机中的私密照片被曝光的事件，这些都是手机木马软件的杰作。2007 年，国内市场上有公司非法销售一款名为“X 卧底”的手机间谍软件，可以全面监视手机短信、通信记录等，并具有远程窃听功能等。从技术的角度来看，这种软件实际上就是一种木马程序，它可以很容易地将用户手机变成窃听器，导致用户信息的泄露。

② 造成用户经济损失。很多手机病毒会强制被感染手机不断地向外发送彩信或拨打电话，给用户造成经济损失，恶意的手机病毒制造者还会借此赚取不义之财。2007 年在俄罗斯出现的“RedBrowser”手机病毒一旦被植入手机并被激活，被感染的手机会在非常隐蔽的状态下向付费号码 1055 发送短信，每条信息的收费为 177 卢布(合 6 美元)，短时间内就会造成用户巨额话费的支出。

③ 破坏手机软硬件。手机病毒最常见的危害就是破坏手机软、硬件，导致手机无法正常工作，典型的症状是手机死机、运行慢、待机时间减短、重启等，一些恶性病毒则能够摧毁手机操作系统，甚至导致内部芯片烧坏。芬兰一家信息安全公司发现的手机病毒“Fontal. a”，是第一种能摧毁“Symbian”手机操作系统的手机病毒，它向手机操作系统植入恶意文件，一旦用户重启手机被感染，该病毒就会导致操作系统崩溃，并且只能通过格

式化并重新安装系统才能修复。

④ 远程控制用户手机。2004年8月发现的后门病毒“Backdoor. Wince. Brador. a”，可以使攻击者远程控制被感染的手机或其他手持设备。该病毒会在被感染设备中开设后门，攻击者利用它不但可以偷窃被感染手机里的电话号码和电子邮件，还可以对其进行远程控制，运行多种危险指令。此类病毒一旦大规模扩散并控制数量巨大的手机，将会成为一种能够对移动通信网络造成破坏的潜在力量。

(2) 对移动通信网络的危害。

手机病毒也能对移动通信网络进行攻击，造成服务中断和网络瘫痪等事故。此类攻击的危害主要表现为：

① 堵塞移动通信服务。某些手机病毒会强制被感染手机不断地向所在通信网络发送垃圾信息或拨打特定服务号码，如果大量被感染的手机在短时间内同时发起此类行为，就会形成拒绝服务攻击(denial of service)，大量占用通信网络资源，堵塞网络通信服务，甚至会让移动通信网络局部瘫痪。

② 控制或使特定网络设施瘫痪。如果黑客们找到了移动通信设备(如短信网关，WAP网关，业务服务器等)的漏洞，就可以利用该漏洞研制出有针对性的手机病毒。一旦攻击成功，或导致设备瘫痪，或控制这些设备为他们服务，将会对整个移动通信网络造成巨大影响，导致重大经济损失，并可能产生社会问题。

4. 防范手机病毒的安全建议

(1) 从手机终端进行防范。

手机终端是手机病毒寄生和发作的温床，防范手机病毒，应首先在手机上做好安全防护。一是提高手机用户的防病毒意识，不接受陌生请求，随时删除可疑短信或彩信，不浏览危险网站，保证下载的安全性等；二是在手机上安装杀毒软件和防火墙等安全软件，过滤收到的信息(短信、彩信和邮件等)和下载的文件，对其内容进行病毒查杀，防止有害的程序安装到手机上。

(2) 在移动通信网络设备处进行防范。

移动通信网是一个受到严格管理的网络，手机病毒的防护重点是在网络层面上实现。因为大部分手机病毒的传播方式需要依靠移动通信网络，运营商进行网络杀毒是最有效的方法，这可以在移动网络设备处(例如GGSN、彩信网关、WAP网关等)对网络行为和信息内容采用安全审计、深度报文检测等技术实现对敏感信息和有害行为的及时发现和过滤，确保传送的内容安全可靠，并及时封堵攻击来源，把危害降到最低。

前面分析的主要是基于DOS和Windows操作系统的病毒，或者统称为微软操作系统病毒。目前市场上除了微软的操作系统以外，还有一些非主流的，但很具发展前景的操作系统，例如Linux、UNIX、MAC OS、FreeBSD、BeOS等。随着嵌入式操作系统在各类电子产品中的应用，一些专门针对这些产品的病毒被黑客制造出来。此前就曾出现过袭击高级轿车、智能手机等设备的蠕虫病毒和木马病毒。在未来数年内，使用各种嵌入式操作系统的电子设备可能会遭到更大规模的病毒袭击。

6.4 计算机病毒的防治

本节主要介绍计算机病毒的预防措施、检测方法与清除方法。

6.4.1 计算机病毒的预防

解决病毒攻击的理想方法是对病毒进行预防，即在第一时间内阻止其进入系统。从原则上讲，计算机病毒防治应采取“主动预防为主、被动处理为辅”的策略。

预防是指采用一定的技术手段，监视、跟踪系统内类似的操作，阻断可能是病毒入侵的行为的发生，提供对系统的保护。预防措施应可以准确、实时地监测由光盘、U 盘、硬盘不同目录之间、局域网、Internet 或其他形式的文件下载等多种方式进行的传输；能够在病毒侵入系统时发出警报，记录携带病毒的文件，及时清除其中的病毒；对网络而言，能够向网络管理员发送关于病毒入侵的信息，记录病毒入侵的工作站，必要时还要能够注销工作站，隔离病毒源。

1. 引导型病毒的预防

引导性病毒一般在启动计算机时，优先获得控制权，强占内存。通常情况下，只要不用软盘或者只用“干净的”软盘启动系统，是不会染上引导型病毒的。对软盘进行写保护，则可以很好地保护软盘不被非法写入，从而不被感染上启动型病毒。但要保护硬盘的安全，除了从操作方面注意外，只有采取用软盘来保护硬盘的措施。

2. 文件型病毒的预防

文件型病毒的预防方法是在源程序中增加自检及清除病毒的功能。这种方法可以使得可执行文件从一生成就具有抗病毒的能力，从而可以保证可执行文件的干净。自检清除功能部分和可执行文件的其他文件融为一体，不会和程序的其他功能冲突，也使得病毒制造者无法造出针对性的病毒来。可执行文件染不上病毒，文件型病毒就无法传播了。

3. 个性化的预防措施

计算机病毒的感染总是带有普遍性的或大众化的，以使计算机病毒范围尽可能地广，所以一些个性化的处理可能对计算机病毒的预防或者免疫具有非常好的效果。如给一些系统文件改名或扩展名；对一些文件甚至子目录加密。使得计算机病毒搜索不到这些系统文件。

4. 日常操作的预防措施

在日常使用计算机的操作过程中，应注意以下几点预防措施：①计算机专人负责、专人管理。②不要从软盘、U 盘、移动硬盘引导系统。③养成经常用杀毒软件检查硬盘、外来文件和每一张外来盘的良好习惯。④不用来历不明的软件，也不要使用非法解密或复制的软件。⑤对游戏程序要严格控制。⑥网络上的计算机用户，要遵守网络的使用规定，

不能随意在网络上使用外来软件。⑦安装病毒防火墙,或在操作系统中进行相关的安全设置,如禁止 Active 控件、禁止自动脚本等。

6.4.2 计算机病毒的检测

计算机检测是指在特定环境中检查是否存在病毒,并能够准确地报告出病毒的名称。检查的对象可以是内存、文件(可执行文件、Word 文件、VBS 文件及其他)、磁盘引导区等。查毒率和误报率是检测病毒的两个重要指标。

下面介绍一些常用的病毒检测方法。

1. 外观检测法

计算机病毒传染系统后,系统会出现一些异常症状,根据其症状可以判定是否中毒以及病毒的类型。计算机中毒后常出现以下症状:

(1) 计算机屏幕上出现异常信息或图形,如大麻病毒在系统启动时提示:"Your PC is stoned",1575 病毒发作时屏幕上出现小毛虫。

(2) 计算机系统的启动或运行速度减慢。

(3) 计算机系统出现异常死机或重启。例如冲击波病毒会导致莫名其妙地死机或重新启动计算机或显示 60 秒倒计时关机。

(4) 系统文件大小发生变化或者丢失。如文件型病毒一般修改文件的字节长度,黑色星期五病毒在破坏条件被触发时将删除执行的文件。

(5) 打印机的打印速度降低或者打印机失控。

(6) 存储容量异常减少。

(7) 系统不能由硬盘引导。

(8) 数据丢失。

(9) 执行异常操作。

(10) 文档奇怪消失,文档内容被加入奇怪资料,文档名称、日期、属性被更改。

2. 比较法

比较法不需要专用的查病毒程序,只要用原始的或正常的系统或文件与被检测的系统或文件进行比较。比较法包括长度比较法、内容比较法、内存比较法、中断比较法等。

(1) 长度比较法及内容比较法。

病毒感染系统或文件,必然引起系统或文件的长度和内容的变化。以长度或内容是否变化作为检测病毒的依据,在许多场合是有效的。但是,只检查可疑系统或文件的长度和内容是不能充分认定被检对象是否被病毒感染。因为:①有些命令(如连接命令)可以引起长度和内容变化,但是合法的。②某些病毒感染文件时,宿主文件长度可保持不变。

上述情况下,长度比较法和内容比较法不能区别程序的正常变化和病毒攻击引起的变化,不能识别保持宿主程序长度不变的病毒,无法判定为何种病毒。实践表明,将长度比较法、内容比较法作为检测病毒的手段之一,与其他方法配合使用,效果更好。

（2）内存比较法。

病毒如果驻留于内存，必须在内存中申请一定的空间，并对该空间进行占用、保护。因此，通过对内存的检测，观察其空间变化，与正常系统内存的占用和空间进行比较，可以判定是否有病毒驻留其间，但无法判定为何种病毒，此法对于那些隐蔽型病毒无效。

（3）中断比较法。

病毒为实现其隐蔽和传染破坏之目的，常采用“截留盗用”技术，更改、接管中断向量，让系统中断向量转向执行病毒控制部分。因此，将正常系统的中断向量与有毒系统的中断向量进行比较，可以发现是否有病毒修改和盗用中断向量。

比较法的优点是简单、方便，不需要专用软件。缺点是无法确认病毒的种类名称。另外，造成被检测程序与原始备份之间差别的原因尚需进一步验证，以查明是由于计算机病毒造成的，或是由于 DOS 数据被偶然原因（如突然停电、程序失控、恶意程序等）破坏的。

3．特征代码扫描法

特征代码扫描法是用每一种病毒体含有的特定字符串对被检测的对象进行扫描。如果在被检测对象内部发现了某一种特定字符串，就表明发现了该字符串所代表的病毒。

（1）病毒扫描软件的组成：

① 病毒代码库，含有经过特别选定的各种计算机病毒的代码串；

② 扫描程序，利用病毒代码库进行扫描的扫描代码串。

（2）特征代码扫描法的优点：

① 当特征串选择正确时，病毒检测软件让计算机用户使用起来方便快速，对病毒了解不多的人也能用它来发现病毒；

② 可识别病毒的名称；

③ 误报警率低；

④ 依据检测结果，可做杀毒处理。

（3）特征代码扫描法的缺点：

① 不能检测未知病毒；

② 搜集已知病毒的特征代码费用开销大；

③ 在网络上效率低（在网络服务器上，因长时间检索会使整个网络性能变坏）；

④ 不能检查多形性病毒；

⑤ 不能对付隐蔽性病毒，因为，隐蔽性病毒如果先进驻内存，后运行病毒检测工具，隐蔽性病毒能先于检测工具，将被查文件中的病毒代码剥去，检测工具的确是在检查一个有毒文件，但它真正看到的却是一个虚假的“好文件”，而不能报警，被隐藏性病毒所蒙骗。

病毒扫描程序能识别的计算机病毒的数目完全取决于病毒代码库内所含病毒的种类有多少。库中病毒代码种类越多，扫描程序能认出的病毒就越多。面对不断出现的新病毒，必须不断更新版本，否则检测工具便会老化，逐渐失去实用价值。病毒特征代码法对未出现过的新病毒，自然无法知道其特征代码，因而无法去检测这些新病毒。

4. 校验和法

将正常文件的内容，计算其校验和，将该校验和写入文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前，应先检查当前文件内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法，它既可以发现已知病毒又可以发现未知病毒。在 SCAN 和 CPAV 工具的后期版本中除了病毒特征代码法之外，还纳入校验和法，以提高其检测能力。

(1) 运用校验和法查病毒通常采用的方法。

① 在检测病毒工具中纳入校验和法，对被查的对象文件计算其正常状态的校验和，将校验值写入被查文件中或检测工具中，而后进行比较。

② 在应用程序中，放入校验和法自我检查功能，使文件正常状态的校验和写入文件本身中，每当应用程序启动时，比较现行校验和与原校验和值，实现应用程序的自检测。

③ 将校验和检查程序常驻内存，每当应用程序开始运行时，自动比较检查应用程序内部或别的文件中预先保存的校验和。

(2) 校验和法的优点。

① 方法简单。

② 既能发现已知病毒，也能发现未知病毒。

③ 被查文件的细微变化也能发现。

(3) 校验和法的缺点。

① 必须预先记录正常态的校验和。

② 会误报警。在比较法中，可以知道病毒感染并非文件内容改变的唯一原因，文件内容的改变有可能是正常程序引起的，但校验和法对文件内容的变化太敏感，不能区分是正常程序引起的变动，还是病毒感染引起的变动，而频繁报警。如已有软件版本更新、变更口令、修改运行参数、校验和法都会误报警。

③ 不能识别病毒类，不能报出病毒名称。

④ 不能对付隐蔽型病毒，隐蔽性病毒进驻内存后，会自动剥去染毒程序中的病毒代码，使校验和法受骗，对一个有毒文件算出正常校验和。

5. 行为监测法

利用病毒特有行为特性来监测病毒的方法，称为行为监测法。通过对病毒多年的观察、研究，有一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现了此类病毒行为，立即报警。

这些作为监测病毒的行为特征如下：

(1) 占有 INT 13H。

所有的引导型病毒，都攻击 Boot 扇区或主引导扇区。系统启动时，当 Boot 扇区或主引导扇区获得执行权时，系统刚刚开工，一般引导型病毒都会占用 INT 13H 功能，因为其他系统功能未设置好，无法利用。

(2) 修改 DOS 系统数据区的内存总量，病毒常驻内存后，为了防止 DOS 系统将其覆

盖，会修改系统内存总量。

（3）对.COM、.EXE文件做写入动作，病毒要感染，必须写COM、EXE文件。

（4）病毒程序与宿主程序的切换，染毒程序运行中，先运行病毒，而后执行宿主程序。在两者切换时，有许多特征行为。

行为监测法的优点是：不仅可以发现已知病毒，而且可以相当准确地预报未知的多数病毒。行为监测法的缺点：可能误报警和不能识别病毒名称，而且实现起来有一定难度。

6. 感染实验法

感染实验法是利用病毒的感染特性根据特定的感染实验检查系统是否中毒。如果系统中有异常行为，最新版的检测工具也查不出病毒时，就可以做感染实验，先运行可疑系统中的程序，再运行一些确切知道不带毒的正常程序，然后观察这些正常程序的长度和校验和，如果发现有的程序增长，或者校验和变化，就可断言系统中有病毒。

由于病毒检测工具落后于病毒的发展，当病毒检测工具不能发现病毒时，如果不用感染实验法，便束手无策。使用感染实验法，可以检测出病毒检测工具不认识的新病毒，可以摆脱对病毒检测工具的依赖，自主地检测可疑新病毒。

7. 软件模拟法

多态性病毒每次感染都改变其病毒密码。对付这种病毒，特征代码法失效。因为多态性病毒代码实施密码化，而且每次所用密钥不同，把染毒的病毒代码相互比较，也无法找出相同的可能作为特征的稳定的代码。虽然行为检测法可以检测多态性病毒，但是在检测出病毒后，因为不知病毒的种类，难以消毒处理。为了检测多态性病毒，可应用新的检测方法——软件模拟法。这是一种软件分析器，用软件方法来模拟和分析程序的运行。

新型检测工具纳入了软件模拟法，该类工具开始运行时，使用特征代码法检测病毒，如果发现隐蔽病毒或多态性病毒嫌疑时，启动软件模拟块，监视病毒的运行，待病毒自身的密码译码以后，再运用特征代码法来识别病毒的种类。

8. 分析法

病毒检测的分析法是反病毒工作中不可或缺的重要技术，任何一个性能优良的反病毒系统的研制和开发都离不开专门人员对各种病毒的详尽而认真的分析。

一般使用分析法的人是反病毒技术人员。使用分析法的目的在于：①确认被观察的磁盘引导区和程序中是否含有病毒。②确认病毒的类型和种类，判定其是否是一种新病毒。③搞清楚病毒体的大致结构，提取特征识别用的字符串或特征字，用于增添到病毒代码库供病毒扫描和识别程序用。④详细分析病毒代码，为制定相应的反病毒措施制订方案。

9. 新一代反病毒检测技术

（1）虚拟机技术。

多态性病毒或多型性病毒，即俗称变形病毒。多态性病毒每次感染后都改变其病毒

密码，这类病毒的代表是幽灵病毒。多态和变形病毒的出现，让传统的特征查毒技术无能为力。之所以造成这种局面，是因为特征查毒技术是对静态文件进行查杀的，而多态和变形病毒只有在开始运行后才显露原形。

虚拟机技术是一种软件分析器，在计算机的虚拟内存中，用软件方法来模拟和分析不明程序的运行。在执行过程中，从虚拟机环境内截获文件数据。如果含有可疑病毒代码，则杀毒后将其还原到原文件中，从而实现对各类可执行文件内病毒的查杀。

(2) 启发式扫描技术。

病毒和正常程序的区别可以体现在许多方面。一个运用启发式扫描技术的病毒检测软件，实际上就是以特定方式实现的动态高度器或反编译器，通过对有关指令序列的反编译逐步理解和确定其蕴藏的真正动机。

在具体实践上，启发式扫描技术是相当复杂的。通常这类病毒检测软件要能够识别并探测许多可疑的程序代码指令序列，这些功能操作将被按照安全和可疑的等级进行排序，并且根据操作特点赋予不同的加权值。如果对于一个程序的加权值的总和超过一个事先定义的数值，那么，病毒检测程序就可以声称“发现病毒”。为减少谎报，最好把多种可疑功能操作同时并发。另外，目标代码的前后逻辑关系也是启发式扫描需要注意的问题。

(3) 主动内核技术。

主动内核技术就是将已经开发的各种网络防病毒技术从源程序级嵌入到操作系统或网络系统的内核中，实现网络防病毒产品与操作系统的无缝连接。主动内核技术的要点在于它采用了与“主动反应装甲”同样的概念，能够在病毒突破计算机系统软、硬件的瞬间发生作用。这种作用，一方面不会伤及计算机系统本身，另一方面却对企图入侵系统的病毒具有彻底拦截并杀除的作用。

反病毒技术从防病毒卡到自升级的软件反病毒产品，再到动态、实时的反病毒技术，都属于被动式的防御理念，其最大的缺点在于将防治病毒的基础建立在病毒侵入操作系统或网络系统以后，作为上层应用软件的反病毒产品，只能借助于操作系统或网络系统所提供的功能来被动地防治病毒。实时化的反病毒技术，可以被称为“主动反应”技术，因为这时反病毒技术能够在用户不关心的情况下，自动将病毒拦截在系统之外。但其不是深入到内核的技术。

在操作系统和网络的内核中加入反病毒功能，使反病毒成为系统本身的底层模块，而不是一个系统外部的应用软件，一直是反病毒专家追求的目标。主动内核技术，就是从操作系统内核这一深度，给操作系统和网络系统本身打了一个补丁，而且是一个“主动”的补丁，这个补丁将从安全的角度对系统或网络进行管理和检查，对系统的漏洞进行修补；任何文件在进入系统之前，作为主动内核的反毒模块都将首先使用各种手段对文件进行检测处理。

(4) 云安全技术。

“云安全”(cloud security)技术是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常进行监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分

析和处理,再把病毒和木马的解决方案分发到每一个客户端。

云安全是一群探针(海量的客户端)的结果上报、专业处理结果的分享,传统的上报是人为的、手动的,而云安全是自动及时上报,由系统自动完成,只要几秒钟。理想状态下,从一个盗号木马攻击某台计算机,到整个“云安全”网络对其进行免疫、查杀,仅需几秒。

6.4.3 计算机病毒的清除

计算机病毒的清除是指从感染对象中清除掉病毒,使其恢复到被感染前的状态。根据不同类型病毒的感染方式,可以采取不同的方法进行恢复。病毒往往有一个潜伏期,在病毒发作之前发现病毒,就可以采取对应措施清除病毒以避免其发作。

1. 清除病毒的方法

(1) 杀毒软件清除法。

清除病毒的主要方法是使用专门的杀毒软件。目前的杀毒软件有两种:一种是针对已知病毒的,虽然这类杀毒产品对病毒的控制起到了很大的作用,但它暴露出来的问题却越来越多。另外一种是新型的启发式杀毒软件,通过模拟最新出现的安全威胁的功能来识别病毒威胁。这方面的杰出杀毒软件代表有东方微点公司的微点主动防御软件,卡巴斯基反病毒软件和360安全卫士。

(2) 重装系统并格式化硬盘。

格式化会破坏硬盘上的所有数据,格式化前必须确定硬盘中的数据是否还需要,一定要先做好备份工作。另外格式化时一般是进行高级格式化,不要轻易进行低级格式化,低级格式化是一种损耗性操作,它对硬盘寿命有一定的负面影响。

(3) 手工清除方法。

手工清除计算机病毒对技术要求高,需要熟悉机器指令和操作系统,难度比较大,一般只能由专业人员操作。

一般来说,病毒在正常模式下比较难清理,所以需要重新启动计算机在安全模式下查杀。顽固的病毒可以通过下载专杀工具来清除,恶劣的病毒可以通过重装系统来彻底清除。

2. 清除病毒的注意事项

在清除病毒的过程中需要注意如下事项:

(1) 杀病毒时用来启动的系统盘要确保无病毒,所用的病毒清除软件或工具软件也必须是无毒的。

(2) 当系统感染了多种病毒时,用病毒清除软件进行一次杀毒以后,可能还未清除全部病毒,特别是引导区病毒,还要进行一至多次杀毒工作才能将病毒全部清除干净,因此需再次杀毒,没有找到病毒的信息后,杀毒工作才算结束。

(3) 进行杀毒处理的文件必须是非打开状态。如果文件打开,应先关闭。如果文件型病毒已驻留内存,在正常模式下,由于带毒的文件正在运行并且可能无法正常关闭,此时是无法对这些文件直接进行操作的,杀毒时遇见“文件正在使用”或者“清除失败”这样

的报告，原因就是如此。

(4) 磁盘上经常会有一些被压缩工具处理过的文件，压缩的目的是为了节省磁盘空间，便于保密与携带。但如果有人无意将病毒传染的文件使用压缩工具压缩了，那么反病毒软件很可能就无法直接将病毒从压缩文件中查出。因此对于压缩文件应先采用解压缩算法对压缩文件进行解压缩后，再进行查病毒和杀病毒处理，这要求杀毒软件支持相应的压缩算法。

(5) 由于文件型病毒会对宿主文件进行修改，把自身代码添加到宿主文件上，所以会造成一些结构比较复杂的文件损坏，如一些自解压的文件(通常是一些软件的安装文件)或一些带有自校验功能的文件无法运行，当它感染了系统文件，还会造成系统的不稳定性，如经常出现“非法操作”等。出现的这些症状即使使用杀毒软件把病毒清除干净了也无法修复被感染的文件。因为文件的某些部分已经被病毒代码覆盖破坏，杀毒软件清除病毒后无法知道程序被感染之前的代码是什么，也就意味着清除这类病毒后，不能保证程序完全被修复。因此，清除病毒不等同于修复文件。

(6) 在清除通过网络传染的病毒时，要断掉网络连接(如拔掉网线)，特别是在局域网中，一定要把所有计算机上的病毒全部都查杀干净以后才可以联网，否则一台刚刚杀过毒的计算机可能被再次感染，这点一定要注意。如果对一个中型或大型的局域网进行病毒处理，应使用网络版的杀毒软件，用单机版效果一般不理想。

(7) 不要使用网页在线杀毒。其原因是很难彻底清除病毒，同时，由于利用了 IE 的特殊功能，会带来更多的安全隐患，而且一般反病毒厂商也不会提供全面的病毒库文件，所以这种方法充其量只能查出计算机上是否感染流行的病毒，而不能有效地进行清除病毒。

(8) 千万不要以为杀毒软件是万能的，不要以为有了正版杀毒软件和最新病毒库就肯定能检测和清除所有的病毒。

6.4.4 常用反病毒软件

利用反病毒软件对病毒进行防治仍然是目前的主要手段。下面介绍几种比较有特点的反病毒软件。

1. 国产反病毒软件

(1) 瑞星杀毒软件。

瑞星杀毒软件是国产杀软的龙头老大，有十几年相关市场经验，其产品占系统资源较多、产品组件较多、杀毒能力表现不很理想，至今未能通过 VB100％测试。唯一的优势是因国内用户较多，故对国内新病毒反应较快。

(2) 金山毒霸。

金山毒霸是金山公司推出的计算机安全产品，监控、杀毒全面、可靠，占用系统资源较少。其软件的组合版功能强大(毒霸主程序、金山清理专家、金山网镖)，集杀毒、监控、防木马、防漏洞为一体，是一款具有市场竞争力的杀毒软件。

(3) 江民杀毒软件。

江民杀毒软件是一款老牌的杀毒软件。它具有良好的监控系统，独特的主动防御使

不少病毒望而却步。建议与江民防火墙配套使用。作者在多次病毒测试中，发现江民的监控效果非常出色，可以与国外杀毒软件相媲美。它占用资源不是很大，是一款不错的杀毒软件。另外江民 2009 与 360 安全卫士有冲突，建议选择其一安装。

（4）360 杀毒软件。

360 杀毒是 360 安全中心出品推出的一款永久免费，性能超强的云安全杀毒软件，在中国市场占有率第一。360 杀毒具有查杀率高、资源占用少、升级迅速等优点。

360 杀毒采用领先的五引擎：国际性价比排名第一的 BitDefender 引擎＋修复引擎＋360 云引擎＋360QVM 人工智能引擎＋小红伞本地内核，强力杀毒，可以全面保护计算机安全，拥有完善的病毒防护体系，且唯一真正做到彻底免费、无须任何激活码。360 杀毒轻巧快速、查杀能力超强、独有可信程序数据库，防止误杀，误杀率远远低于其他杀毒软件，依托 360 安全中心的可信程序数据库，实时校验，为计算机提供全面保护。最新版本特有全面防御 U 盘病毒功能，彻底剿灭各种借助 U 盘传播的病毒，第一时间阻止病毒从 U 盘运行，切断病毒传播链。

（5）360 安全卫士。

360 安全卫士是 360 安全中心出品推出的一款永久免费、功能强、效果好、受用户欢迎的上网安全软件。360 安全卫士拥有查杀木马、清理插件、修复漏洞、电脑体检、保护隐私等多种功能，并独创了“木马防火墙”、“360 密盘”等功能，依靠抢先侦测和云端鉴别，可全面、智能地拦截各类木马，保护用户的账号、隐私等重要信息。

360 杀毒和 360 安全卫士配合使用，是安全上网的“黄金组合”。360 安全卫士软件硬盘占用很小，运行时对系统资源的占用也相对较低，是一款值得普通用户使用的较好的安全防护软件。

2. 国外反病毒软件

（1）诺顿杀毒软件。

诺顿是由 Symantec 公司出品的一款杀毒软件，包括网络版和专业版，单机防病毒既可以使用网络客户端程序，也可以使用专业版。它可以自动对计算机磁盘中的文件及 Internet 电子邮件进行监测/扫描，及时查杀病毒，以保证计算机的安全。

（2）NOD32。

国外权威的防病毒软件评测给了 NOD32 很高的分数，其在全球共获得超过 40 多个奖项，是全球唯一一个通过 26 次 VB100％测试的防毒软件。其产品线很长，几乎支持各种操作系统，可以对邮件进行实时监测，占用内存资源较少，清除病毒的速度和效果都令人满意。缺点是在防侦测方面做得并不是很好，常被病毒破坏，升级慢，而且对国内新病毒反应较慢。

（3）熊猫卫士。

熊猫卫士杀毒终结者的主要技术特色有自我诊断和对防病毒软件自身文件及配置的保护：确保防病毒系统随时正常运行；检测和清除新的安全隐患：愚弄、拨号器、恶作剧、黑客工具；对 E-mail 的完整保护：保护 Outlook Express、Hotmail 和 MSN；拥有 SmartClean2 技术的新一代防病毒软件：自动修复病毒对操作系统配置的破坏（如蠕虫、

木马）等。

(4) 卡巴斯基杀毒软件。

卡巴斯基是俄罗斯民用最多的杀毒软件，卡巴斯基有很高的警觉性，它会提示所有具有危险行为的进程或者程序，因此很多正常程序会被提醒确认操作。

卡巴斯基提供了所有类型的抗病毒防护，包括抗病毒扫描仪、监控器、行为阻断和安全检验等。它几乎支持所有普通操作系统、E-mail 通路和防火墙。卡巴斯基控制所有可能的病毒进入端口。缺点是杀毒速度慢，占用系统资源多，杀毒时尤其明显，系统内存过低时容易导致死机。

(5) 小红伞

一款德国著名杀毒软件的中文昵称，其英文名为 AntiVir，自带防火墙（S 版），它能有效地保护个人计算机以及工作站的使用，以免受到病毒侵害。软件只有几兆大小，它却可以检测并移除超过 60 万种病毒，支持网络更新。

Avira 防毒特性：硬件的等级需求度并不高，所消耗的硬件资源低。软件的病毒定义档更新快速，是每天更新定义档。加强以往的操作系统的背景扫描，有效提高系统防护能力。增加浏览器对网页链接扫描功能，有效提高网页防护。

3. 手机反病毒软件

(1) QQ 手机管家。

QQ 手机管家是一款完全免费的手机安全与管理软件。覆盖了四大智能手机平台，提供系统、通信、隐私、软件、上网五大安全体系；防病毒、防骚扰、防泄密、防盗号、防扣费五大防护功能。QQ 手机管家与卡巴斯基合作提供双核引擎并自主研发强大的云端查杀，独创智能拦截防骚扰，整合 QQ 同步助手打造永不丢失的通讯录，内置手机令牌保护 QQ 账号，为手机终端提供全方位的安全保护与贴心管理。

(2) 360 手机卫士。

360 手机卫士是一款完全免费的手机安全软件，目前市场份额已超过 50%，是中国使用人数最多的手机安全软件。集防垃圾短信，防骚扰电话，防隐私泄露，手机杀毒，对手机进行安全扫描，软件安装实时检测，联网行为实时监控，长途电话 IP 自动拨号，系统清理手机加速，祝福闪信/短信无痕便捷发送，号码归属地显示及查询等功能于一身。

(3) 瑞星杀毒手机软件。

支持系统：Symbian S60、UIQ、WindowsMobile

瑞星杀毒软件允许初始化查杀智能设备上的病毒，查杀病毒先查杀所有正在运行的进程，保证正在运行的病毒能够被清除，再扫描设备中的文件。用户也可单独置顶查杀目录、查杀文件类型等相关信息。但是目前瑞星杀毒软件对实时监控的支持并不是特别理想。

短信/电话防火墙和进程管理器功能是该软件的一大特色，通过设置黑名单，可以实现防御垃圾短信、阻止恶意号码来电等功能。进程管理则可以查看系统当前进程信息、进程的线程信息，用户可以用此方法结束某些恶意程序。

6.5 应用实例

本节主要介绍网页病毒的制作与清除、U 盘病毒的防治、染毒文件的恢复以及反病毒软件 4 个应用实例，说明病毒防治的具体方法。

6.5.1 脚本病毒的制作与清除

Windows 系统的配置信息都写在注册表中，许多脚本病毒就是通过操作注册表来改变和控制系统行为的。

1. 病毒修改注册表的原理

用 VBScript 修改注册表，必须先创建一个能与操作系统沟通的对象，再利用该对象的各种方法对注册表进行操作。创建这个对象的方法和格式如下：

```
Dim OperationRegistry
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
```

上述代码创建了一个能与操作系统沟通的对象 OperationRegistry。

通过这个对象，可以对注册表进行读、写和删除操作。该对象具有的方法包括对注册表的读操作 RegRead、对注册表的写操作 RegWrite 以及对注册表的删除操作 RegDelete。此外。WSH 还有两个通用的方法：WScript. Echo()和 WScript. Quit()。前者用来显示一串文本信息，相当于 VB 中的 MsgBox()；后者用来退出 VBScript 程序。

以上三种操作 RegRead、RegWrite、RegDelete 都需要带参数，尽管这些操作的参数个数和形式不尽相同，但它们都有一个共同且必不可少的参数就是“路径参数”，这里的“路径”是指注册表中的根键和主键。

RegRead 主要是用来读取注册表中主键的默认值或键值，例如：

```
Read_Data1=OperationRegistry.RegRead("HKCR\xxx\")
```

上述代码读取根键 HKEY_CLASSES_ROOT 之下的 xxx 主键的默认值，并将该数据送至变量 Read_Data1。

RegWrite 用来在注册表中新建主键或键值，并赋予它们一个初始值。该操作同样可以修改注册表中已经存在的主键或键值的数据。它需要路径参数、类型参数和初始值。初始值参数对于 RegWrite 操作来说是必不可少的，它可以为空(null)但却不能省掉。在新建主键时，初始值参数给该主键赋予默认值；初始值的类型则是由类型参数决定的。类型参数有以下三个选项：

(1) REG_SZ：字符型。该类型为默认类型。

(2) REG_DWORD：双字节型。

(3) REG_BINARY：二进制型。

例如：OperationRegistry. RegWrite “HKCR\xxx\value”，1，“REG_DWORD”，表示

在主键 xxx 之下新建一个 REG_DWORD 型的键值 value，并置其初始值为 1。

RegDelete 主要是用来删除注册表已存在的主键或键值。同 RegWrite 操作类似，它需要指定键路径。

2. 脚本病毒的制作与运行

制作脚本病毒是为了创建一个病毒，说明病毒的作用，本病毒可以改变系统的“开始”菜单，禁用查找、运行和关闭功能。这只是一个简单的 VBS 文件，将其镶嵌到常用的脚本程序中，病毒就变得复杂了。

制作脚本病毒的步骤如下所述：

第 1 步：编制网页病毒程序。

（1）打开记事本，输入如下命令代码：

```
'脚本文件名 ChangeStartMenu.vbs
Sub Change(Argument)
ChangeStartMenu.RegWrite RegPath&Argument,Key_Data,Type_name
MsgBox("Success")
End Sub
Dim ChangeStartMenu
Set ChangeStartMenu=WScript.CreateObject("WScript.Shell")
RegPath="HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\"
Type_name="REG_DWORD"
Key_Data=1
StartMenu_Run="NoRun"
StartMenu_Find="NoFind"
StartMenu_Close="NoClose"
Call Change(StartMenu_Run)
'禁用"开始"菜单中的"运行"功能
Call Change(StartMenu_Find)
'禁用"开始"菜单中的"查找"功能
Call Change(StartMenu_Close)
'禁用"开始"菜单中的"关闭"功能
```

（2）关闭计算机防火墙与杀毒软件，并将 VBS 文件默认的打开方式设置为 Windows Script Host 方式打开（修改默认打开方式按照 6.3.3 小节所述操作）。将上述编辑好的代码保存到指定的路径中，如“D:\书稿编辑\第六章\test.VBS”。

第 2 步：运行病毒。

双击打开 test.VBS 文件，操作界面将出现如图 6-8 所示的对话框，此时再单击“开始”菜单，将无法执行“运行”、“查找”、“关闭”的功能。

3. 脚本病毒的查杀

如 6.3.3 节所述，脚本病毒的查杀有多种方法，下面主要叙述两种比较简便的方法。

(1) 禁用文件系统对象“FileSystemObject”。

在任务栏中，单击“开始”菜单，打开“运行”命令框，在运行命令对话框中输入“regsvr32 scrrun.dll/u”。单击【确定】按钮，如图 6-9 所示。

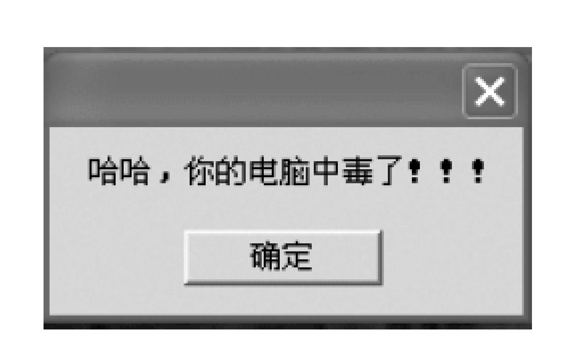


图 6-8　病毒对话框界面



图 6-9　“运行”命令框

(2) 删除 VBS、VBE、JS、JSE 文件后缀名与应用程序的映射。

打开“我的电脑”，单击“工具”菜单，选择“文件夹选项”，单击“文件夹选项”对话框中“文件类型”标签，然后找到扩展名为 VBS 的文件类型(如图 6-10 所示)。单击【更改】按钮，将其打开方式修改为以记事本打开(如图 6-11 所示)，单击【确定】按钮。



图 6-10　文件类型界面



图 6-11　修改打开方式界面

6.5.2　U 盘病毒的防治

1. U 盘病毒的特点

U 盘病毒又称 auto 病毒，是通过 autorun.inf 文件使用户所有的硬盘完全共享或中木马的病毒。经常使用光盘的用户都知道，很多光盘被放入光驱后就会自动播放，计算机要做到这点，需要两个文件：一是光盘上的 autorun.inf 文件，另一个是操作系统本身的系统文件之一的 cdvsd.vxd。cdvsd.vxd 会随时检测光驱中是否有放入光盘的动作，如果

有，便开始寻找光盘根目录下的 autorun.inf 文件。如果存在 autorun.inf 文件则执行其文件中预设的程序。当然，autorun.inf 不光能让光盘自动运行程序，也能让硬盘自动运行程序，病毒程序也正是利用了这一点。

U 盘病毒最大的特征是打开“我的电脑”后，无论双击哪个磁盘，都无法打开，没有任何反应，除这点之外，U 盘病毒还具有如下特点：

① 在系统中占用大量 CPU 资源。

② 在每个分区下建立 autorun.exe 和 autorun.inf 文件，双击该盘符时显示自动运行，但无法打开该分区。

③ 大部分通过 U 盘、移动硬盘等存储设备传播。

④ 可能会引起部分操作系统崩溃，表现在开机自检后反复重启，无法进入系统。

⑤ 当插入 U 盘时自动播放对话框中的第一选项就不再是播放而是运行这个盘中的程序。

2. U 盘病毒的清除

下面通过实例说明清除 U 盘病毒的步骤。

第 1 步：在安全模式下启动系统。

(1) 开机按 F8 键，进入 Windows 安全模式启动界面，如图 6-12 所示。

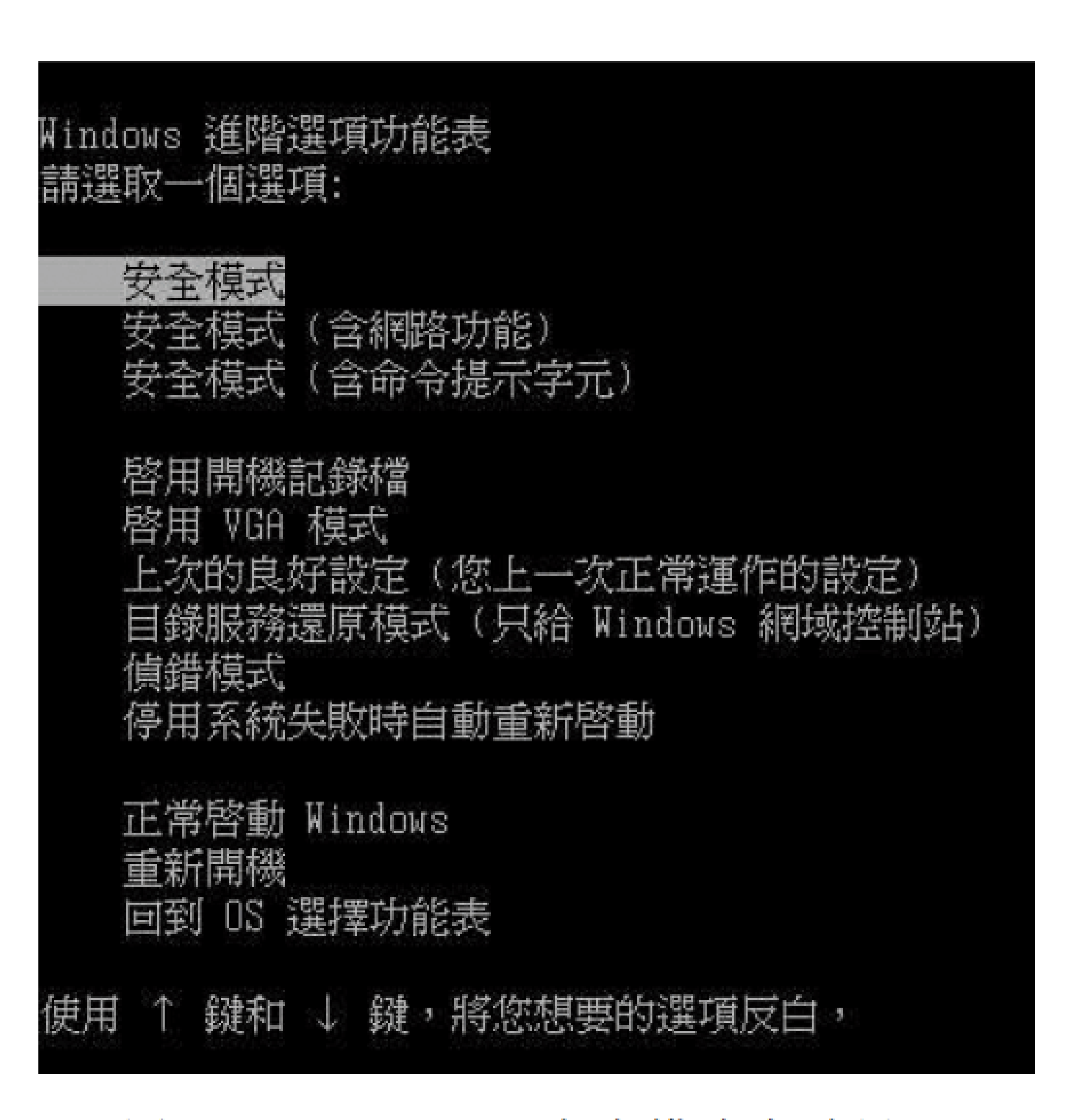


图 6-12　Windows 安全模式启动界面

(2) 选择“安全模式”，然后按 Enter 键，这样系统就通过安全模式启动了。

第 2 步：设置系统显示隐藏文件。

(1) 打开“我的电脑”，选择“工具”→“文件夹选项”命令，如图 6-13 所示。

(2) 在“文件夹选项”对话框中的“查看”标签下勾选掉“隐藏受保护的操作系统文件(推荐)”选项，同时选择下面的“显示所有文件和文件夹”，单击【确定】按钮，如图 6-14 所示。

第 3 步：删除病毒文件。

删除各磁盘根目录中的 autorun.inf 以及病毒文件。



图 6-13　打开“文件夹选项”界面

第 4 步：删除注册表中的启动键值。

(1) 在“开始”菜单中的“运行”栏中输入“regedit.exe”打开注册表，单击【确定】按钮，如图 6-15 所示。

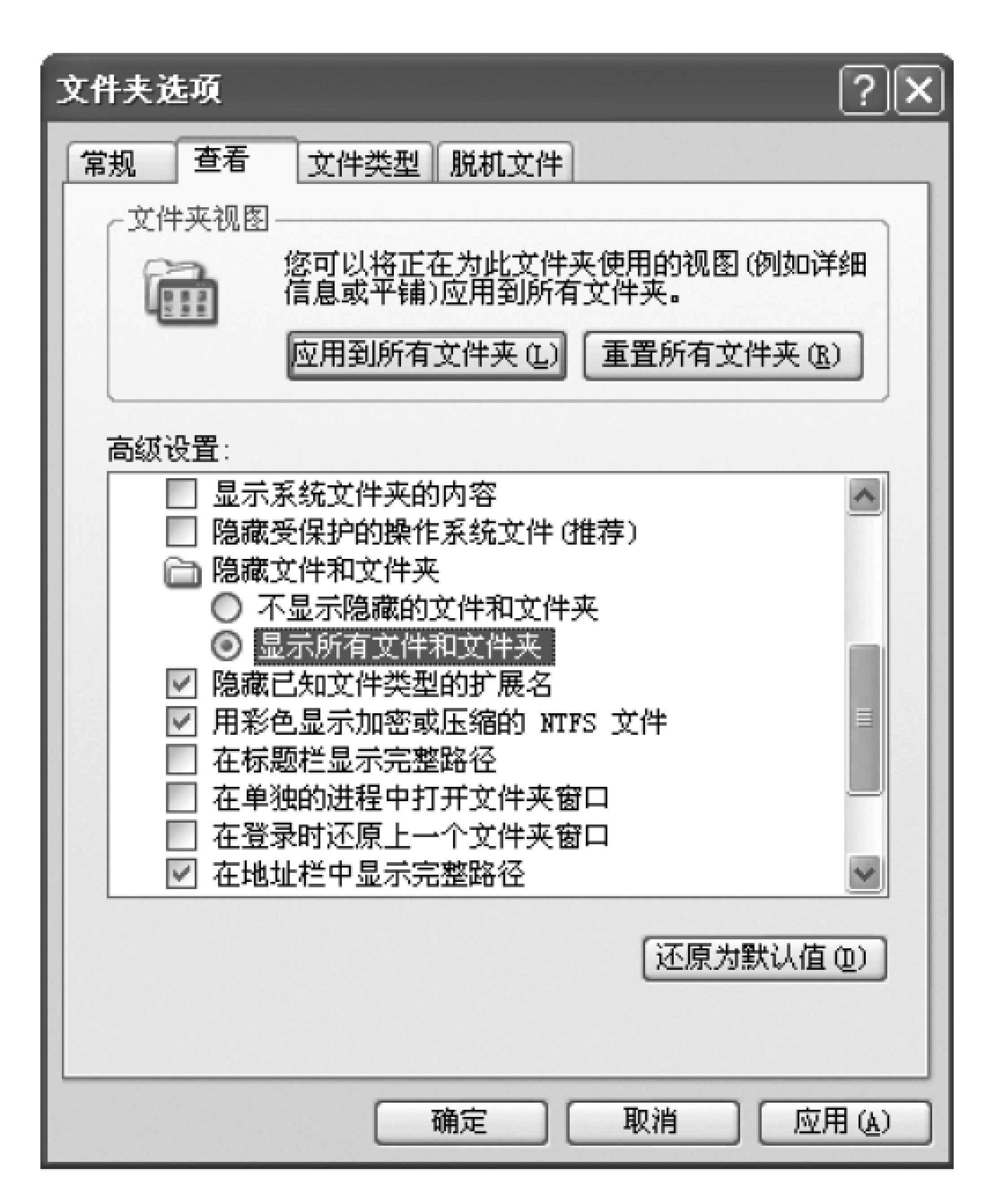


图 6-14　文件夹选项的查看界面



图 6-15　“运行”命令框

(2) 打开注册表后，单击“编辑”菜单中“查找”选项，输入 autorun.inf 文件中记录的内容(如 autorun.exe)，如图 6-16 所示。

(3) 在查找的过程中，删除对应的注册表键值项以及对应路径的文件。最后，重新启动计算机即可。



图 6-16　注册表编辑器“查找”文件界面

3. U 盘病毒的防范

通过以上的操作，可以很容易就能够总结对于 U 盘病毒的防范一般有以下几种方法。

(1) 改变双击习惯。

通常情况下，当打开磁盘分区或移动硬盘时，都是用双击盘符的方法，但这样遇到自动播放病毒时，便会执行病毒程序，所以请用户养成使用鼠标右键打开的习惯，这样，即便遇上自动播放病毒，也能打开各磁盘分区。还有一种方法是，打开“我的电脑”后，单击工具栏上的“文件夹”，用资源管理器的方式查看和使用各磁盘分区。

(2) 使用 U 盘的习惯。

在使用 U 盘时，按住 Shift 键的同时，插入 USB 接口，直到“我的电脑”中显示 U 盘盘符，此方法可阻止 U 盘上的病毒传播到系统中。

(3) 删除 U 盘中的病毒。

用上述中的方法插入 U 盘，然后打开 WinRAR 软件(压缩软件)，并用其打开 U 盘，可查看其中的隐藏文件，删除所有隐藏的文件(一般情况下，U 盘中只有一个“Recycler”文件夹，即回收站的文件夹，其他的隐藏文件都可以删除)。

(4) 下载 U 盘专杀工具。

目前常用的 U 盘专杀工具有 USBkiller、USBcleaner、金山 U 盘专杀工具、pre-scan 四种。USBkiller 能够查杀 auto.exe、AV 终结者、rising 等上百种顽固 U 盘病毒，保证 95%以上的查杀率。免疫功能可以让你制作自己的防毒 U 盘，防止他人使用 U 盘、移动硬盘盗取计算机的重要资料；解除 U 盘锁定状态，解决拔出时无法停止设备的问题；进程管理让你迅速辨别并终止系统中的可疑程序。USBcleaner 是一种纯绿色的辅助杀毒工具，支持简体与繁体语言系统，独有的分类查杀引擎具有检测查杀 470 余种 U 盘病毒，U

盘病毒广谱扫描，U 盘病毒免疫，修复显示隐藏文件及系统文件，安全卸载移动盘盘符等功能，全方位一体化修复杀除 U 盘病毒。同时 USBCleaner 能迅速对新出现的 U 盘病毒进行处理。金山 U 盘专杀工具是金山安全实验室分析了众多 U 盘病毒的规律，开发出的新版专杀工具，可以智能分析，启发判断，通杀未知 U 盘病毒。同时，可以提供病毒免疫功能，阻止新 U 盘病毒的再次感染。对主要通过 U 盘传播的 conficker 病毒有很好的清除能力。pre-scan 是在启动计算机但未登录计算机时，在 Native 环境下运行的病毒专杀工具。不同于普通的专杀，这是一款全新模式的病毒专杀工具，能比较好地解决顽固病毒在计算机启动后无法清除的问题。

6.5.3 染毒计算机的数据恢复

计算机中毒以后，硬盘上的很多数据被恶意删除，在很多情况下硬盘无法启动，致使数据无法读出，此时可以用数据恢复软件将中毒硬盘上的数据恢复出来。其中 EasyRecovery、FinalData、GetDataBack、R-studio 是最有名的几个，下面以 EasyRecovery 为例简单介绍数据恢复的方法。

在硬盘引导区损坏或中了病毒无法启动系统的时候，用 EasyRecovery 可以找回硬盘上的数据。为了提高数据的修复率，在修复前不要再对要修复的分区或硬盘进行新的读写操作，如果要恢复的分区恰恰是系统启动分区，那就马上退出系统，用另一个硬盘来启动系统。然后再运行 EasyRecovery 进行修复。

对于被删除的数据可以通过下列步骤进行恢复：

第 1 步：选择文件被删除的分区。

（1）进入 EasyRecovery 主界面，单击左面【数据恢复】按钮，然后选择右侧的“删除恢复”选项，如图 6-17 所示。



图 6-17 “数据恢复”界面

（2）软件会自动扫描一下系统，稍等一会儿后出现选择分区界面，如图 6-18 所示。左面是选择分区，被删除的文件本来是在哪个分区的，那么就选择哪个分区，如果 C 盘、D 盘、E 盘都有被误删的文件，不能一下全部恢复，需要重复以上的步骤。

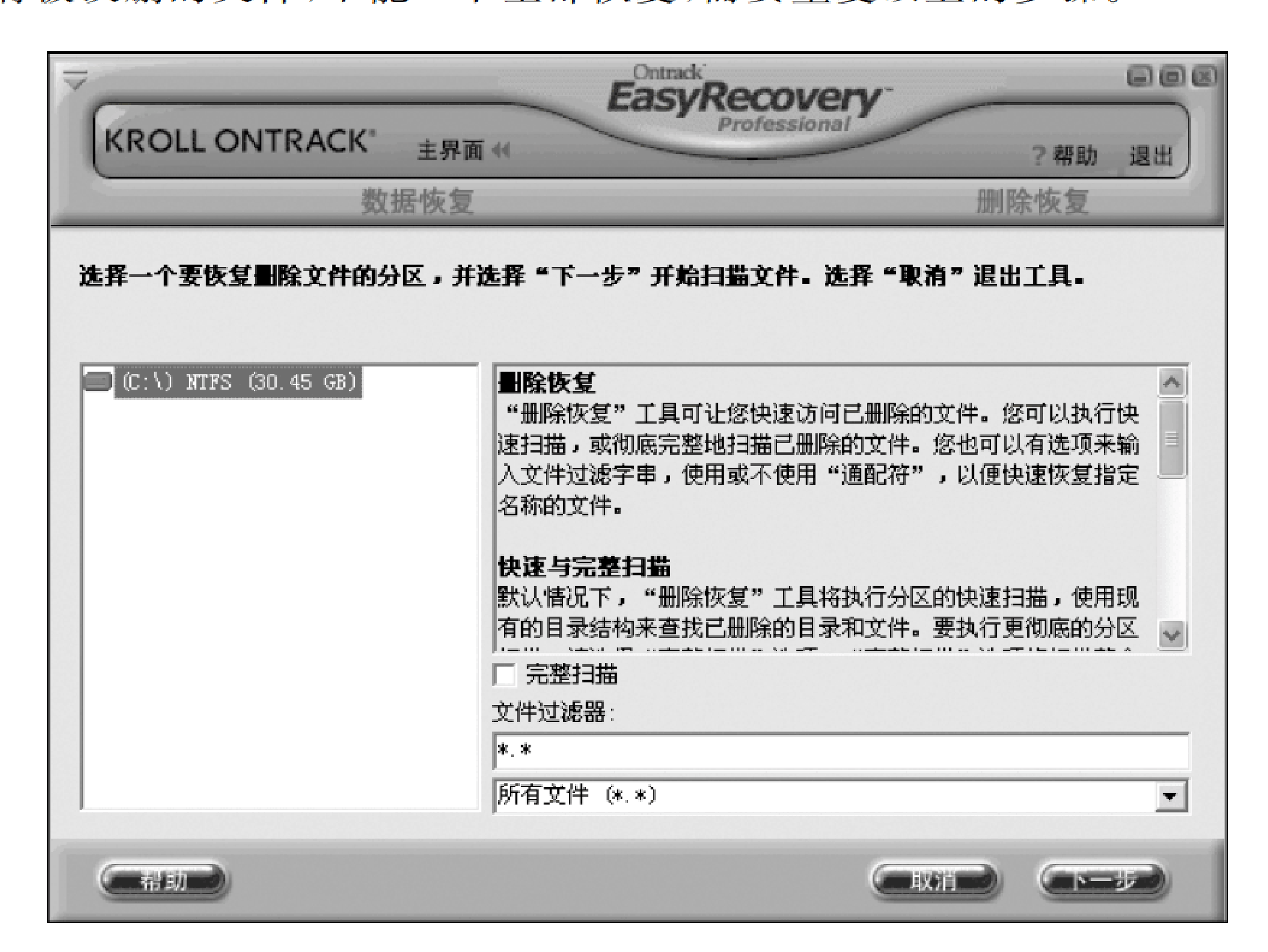


图 6-18　选择分区界面

右边的全面扫描选项一般不要选择，如果接下来恢复数据时发现不是所有被删除的文件都能恢复，那么可以选择这个选项再重新恢复一遍。

第 2 步：找出删除文件。

（1）假设 C 盘中的文件被误删除了，选择 C 盘，单击【下一步】按钮，就会扫描要恢复的文件，时间比较长，主要是根据要恢复分区的大小来决定的，如图 6-19 所示。

（2）经过一段时间的扫描，程序会找到被删除的数据，出现在数据恢复对话框中，如图 6-20 所示，在左边方框内用鼠标单击一下，显示所有找到的可以恢复的数据。

（3）在右边文件列表中勾选要恢复的文件，然后单击【下一步】按钮。

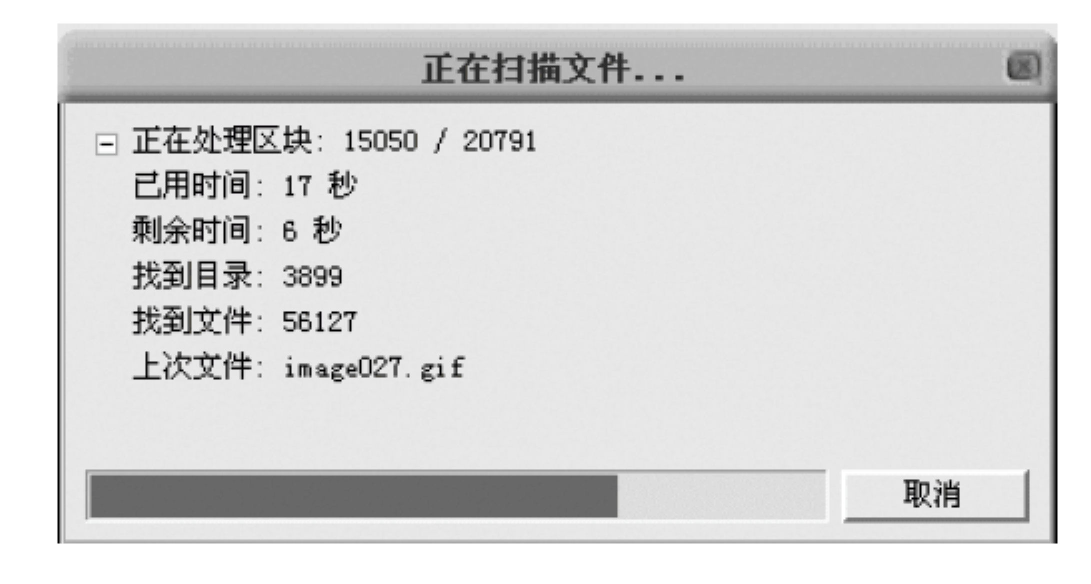


图 6-19　扫描显示框

第 3 步：恢复删除文件。

想要恢复的数据可以备份到硬盘、文件夹或 FTP 服务器上，还可以将数据备份到一个 ZIP 压缩包内。

（1）在系统主界面“恢复统计”框中会提示恢复文件的数量和大小，如图 6-21 所示。根据其大小，在“恢复目的地选项”下拉选项中选择恢复文件备份的存放位置，可以是硬盘、ZIP 压缩包或 FTP 服务器，然后，单击【下一步】按钮。顺便提示一下，不要将恢复的数据放在被删除文件的盘内。否则，很可能发生错误，或者数据不能完全被恢复。



图 6-20　标记文件恢复屏幕



图 6-21　“复制目的地”屏幕

(2) 接下来程序就会恢复所选的硬盘数据，恢复完毕后，到相应的位置内就可以找到所要的数据，如图 6-22 所示。

如果硬盘的数据被格式化，选择“数据恢复”的“格式化恢复”选项，按照以上同样的步骤也可以将丢掉的数据找回来。

6.5.4　使用 360 安全卫士预防查杀病毒

下面简要介绍使用 360 安全卫士的方法。



图 6-22　数据恢复完成界面

1. 360 安全卫士的下载与安装

360 安全卫士为免费使用软件，可从 360 的官方网站（www.360.cn）下载获得。下载的 inst.exe 软件为在线安装程序。运行 inst.exe 安装程序时，要保持网络的畅通，安装程序将在线从 360 官方服务器下载并安装 360 安全卫士，安装界面如图 6-23 所示。



图 6-23　360 安全卫士安装界面

2. 360 安全卫士的升级

360 安全卫士的升级是每次启动时自动完成的，在任务栏中单击“”图标，启动 360 安全卫士，系统自动完成升级，如图 6-24 所示。



图 6-24　360 安全卫士主界面

3．360 安全卫士的使用

（1）电脑体检。

利用 360 安全卫士可以对电脑进行体检，给出当前电脑体检分数，并给出不安全的因素及解决方案。在 360 安全卫士主界面单击【常用】按钮，选择“电脑体检”标签，可以看到当前电脑的体检分数，其界面如图 6-25 所示。



图 6-25　利用 360 安全卫士对计算机进行体检

（2）查杀木马。

启动 360 安全卫士后，在 360 安全卫士主界面单击【常用】按钮，选择“查杀木马”标签，其界面如图 6-26 所示。



图 6-26 360 查杀木马的功能界面

查杀木马有三种方式，快速扫描、全盘扫描、自定义扫描。单击【全盘扫描】按钮，将开始扫描与查杀木马，如图 6-27 所示。



图 6-27 “全盘扫描”木马界面

查杀流行木马操作过程依据硬盘上文件多少所需时间不同，一般需要十几或几十分钟。查杀木马完成后，系统会提示木马名称、路径等信息。

(3) 清理插件。

利用该项功能，可扫描检查系统存在的插件，并给出是否清除建议，供用户选择是否清除，对于恶评插件会单独列出。

在 360 安全卫士主界面单击【常用】按钮，选择“清理插件”标签，从中单击【开始扫描】按钮，如图 6-28 所示，将开始清理插件。



图 6-28　清除插件的功能界面

(4) 修复漏洞。

360 安全卫士具有漏洞修复功能，可自动扫描检查当前计算机系统存在的漏洞，并自动到相应软件的官方发布网站下载和安装漏洞的修复补丁。

(5) 清理垃圾。

360 安全卫士具有清理垃圾功能，可清除系统临时文件、系统缓存文件、无效的快捷方式等无用文件释放磁盘空间。

(6) 清理痕迹。

360 安全卫士具有清理痕迹功能，可对用户的上网历史记录进行清除。

(7) 系统修复。

木马和病毒入侵计算机系统后，通常会对 IE 浏览器、注册表、域名解析文件、文件关联等进行修改。360 提供有系统修复功能，可实现全面的修复处理，让其恢复原状。

(8) 功能大全。

360 安全卫士提供了一系列对系统安全、系统故障诊断或优化系统运行速度的实用工具，在 360 安全卫士主界面单击【常用】按钮，选择“功能大全”标签，可以看到如图 6-29 所示界面，用户可从中选择所需的实用工具。



图 6-29　功能大全界面

(9) 木马防火墙。

通过 360 安全卫士开启“木马防火墙”，保护用户的计算机。

(10) 杀毒。

通过 360 安全卫士可以启动“360 杀毒”软件，实现对系统的杀病毒扫描。

(11) 网盾。

360 安全卫士提供了“360 网盾”，实现对用户上网的全方位的安全防护，可以拦截欺诈网站，拦截木马网站，自动标识百度、谷歌等搜索结果网站的危险程度和欺诈钓鱼网站，可以过滤广告。

360 安全卫士是一款能全方位抵御木马病毒的安全防护软件，有了它，对木马病毒的防御和清除就变得简单多了。

6.6　案例讨论

计算机病毒发展到现在，有很多影响比较大的病毒事件，下面介绍莫里斯蠕虫、CIH 病毒以及熊猫烧香三个典型案例。

案例 6-1　“蠕虫”病毒

1988 年冬天，正在康乃尔大学攻读一年级研究生的莫里斯，把一个被称为“蠕虫”的计算机病毒送进了美国最大的计算机网络——互联网。1988 年 11 月 2 日下午 5 点，互联网的管理人员首次发现网络有不明入侵者。它们仿佛是网络中的超级间谍，狡猾地不断截取用户口令等网络中的“机密文件”，利用这些口令欺骗网络中的“哨兵”，长驱直入互

联网中的用户计算机。入侵得手，立即反客为主，并闪电般地自我复制，抢占地盘。

用户目瞪口呆地看着这些不请自来的神秘入侵者迅速扩大战果，充斥计算机内存，使计算机莫名其妙地“死掉”，只好急如星火地向管理人员求援，哪知，他们此时已经四面楚歌，也只能眼睁睁地看着网络中计算机一批又一批地被病毒感染而“身亡”。当晚，从美国东海岸到西海岸，互联网用户陷入一片恐慌。到 11 月 3 日清晨 5 点，当加州伯克利分校的专家找出阻止病毒蔓延的办法时，短短 12 小时内，已有 6200 台采用 UNIX 操作系统的 SUN 工作站和 VAX 小型机瘫痪或半瘫痪，不计其数的数据和资料毁于这一夜之间。造成一场损失近亿美元的空前大劫难！

这就是在互联网传播的第一种蠕虫病毒，这个程序只有 99 行，利用 UNIX 系统中的缺点，用 Finger 命令查联机用户名单，然后破译用户口令，用 Mail 系统复制、传播本身的源程序，再编译生成代码。最初的网络蠕虫设计目的是当网络空闲时，程序就在计算机间“游荡”而不带来任何损害。当有计算机负荷过重时，该程序可以从空闲计算机“借取资源”而达到网络的负载平衡。而莫里斯蠕虫不是“借取资源”，而是“耗尽所有资源”。

案例 6-2　CIH 病毒

1999 年 4 月 30 日上午，在军方人员的护送下，正在台湾军中服役的 CIH 计算机病毒作者陈盈豪被带到了台北“刑事局”接受警方的侦讯。

陈盈豪从大学一年级开始就痴迷上了计算机，每天都要上网，下载最热门的软件、游戏，因此也经常遭遇计算机病毒。为了解决计算机屡屡“中毒”的烦恼，他看报纸，买了不少广告做得天花乱坠的防病毒软件，结果往往什么用也没有，于是觉得自己被欺骗了。而 CIH 病毒完全是他一人设计的，目的是想出一家公司在广告上吹嘘“百分之百”防毒软件的洋相。他一共设计了五个版本 CIH 病毒，其中 V1.0、V1.1 两个版本没有流出去，而这次危害世界各国的病毒是 V1.2 版。病毒发作的时间之所以定在 4 月 26 日，因为那是他的高中座号，也是他的绰号。

1998 年 6 月 2 日台湾传出首例 CIH 病毒报告。6 月 6 日发现 CIH V1.2 版本。6 月 12 日：发现 CIH V1.3 版本。6 月 26 日 CIH V1.3 版本造成一定程度的破坏。6 月 30 日发现 CIH V1.4 版本。7 月在 INTERNET 环境中发现一个基于 Windows 98 系统的分布感染实例。7 月 26 日 CIH 病毒开始在美国大面积传播。8 月在 Wing Commander 游戏站点发现 DEMO 被感染。两家欧洲的 PC 游戏杂志光盘被发现感染 CIH。8 月 26 日 CIH 1.4 版本爆发，首次在全球蔓延。8 月 31 日：我国公安部发出紧急通知，新华社、中央台新闻联播全文播发。9 月 Yamaha 为某个类型的 CD-R 驱动编写的软件被感染 CIH。10 月一个在全球发行的游戏 SiN 的 DEMO 版被发现感染 CIH。

1999 年 3 月 CIH 1.2 版本被发现在 IBM 的 Aptiva 计算机中预装。

1999 年 4 月 26CIH 1.2 版本首次大范围爆发，全球超过 6 千万台计算机被不同程度地破坏。

2000 年 4 月 26CIH 1.2 版本第二次大范围爆发，全球损失超过十亿美元。

2001 年 4 月 26CIH 第三次大范围爆发。仅北京就有超过六千台计算机遭 CIH

破坏。

2002 年 4 月 26 日 CIH 病毒再次爆发，数千台计算机遭破坏。

2003 年 4 月 26 日仍然有 100 多个 CIH 病毒的受害者。

案例 6-3 “熊猫烧香”病毒

湖北省武汉市李俊于 2006 年 10 月 16 日编写了“熊猫烧香”病毒，并在网上广泛传播，由于中毒计算机的可执行文件会出现“熊猫烧香”图案，如图 6-30 所示，被称为“熊猫烧香”病毒。他以自己出售和他人代卖的方式，在网络上将该病毒销售给 120 余人，非法获利 10 万余元。经病毒购买者进一步传播，导致该病毒的各种变种在网上大面积传播，对互联网用户计算机安全造成了严重的破坏。



图 6-30 “熊猫烧香”图案

“熊猫烧香”原病毒只会对 EXE 图标进行替换，并不会对系统本身进行破坏。而大多数用户中的是变种病毒，用户计算机中毒后会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象。该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致企业局域网瘫痪，无法正常使用。“熊猫烧香”能感染系统中 exe，com，pif，src，html，asp 等文件，能终止大量反病毒软件的进程并且会删除扩展名为 gho 的文件，该文件是系统备份工具 GHOST 的备份文件，使用户的系统备份文件丢失。被感染的用户系统中所有.exe 可执行文件全部被改成熊猫举着三根香的模样。该病毒盗取用户游戏账号、QQ 账号进而使计算机用户造成损失。

2006 年底，“熊猫烧香”病毒及其变种在我国互联网爆发，它传播速度快，危害范围广，超过上百万个人用户、网吧及企业局域网用户遭受感染和破坏，引起社会各界高度关注，日本、德国等国家，纷纷发布“熊猫烧香”的预防警报。《瑞星 2006 安全报告》将其列为十大病毒之首，在《2006 年度中国大陆地区电脑病毒疫情和互联网安全报告》的十大病毒排行中一举成为“毒王”。

根据三个案例，讨论病毒制造者编写病毒原因，能否从源头杜绝病毒。

归纳总结

1. 阅读本章内容，可以看出计算机病毒的危害性是相当大的。归纳总结病毒有哪些危害，说明如何才能将病毒危害减到最小。

2. 讨论除了反病毒技术在对抗病毒中需要及时进步，归纳说明还有哪些方面也需要改进。

3. 归纳总结有哪些类型的病毒，说明计算机病毒会朝着什么方向发展。

思考与实践

思考题

1. 什么是计算机病毒？计算机病毒由哪些组成？
2. 计算机病毒有哪些危害？病毒有哪些传播途径？感染病毒后计算机有哪些症状？
3. 有哪些常见的计算机病毒？它们有哪些特性？
4. 传统的计算机病毒有哪些？如何预防这类病毒？
5. 互联网下有哪些新型病毒？如何预防这类病毒？
6. 如何预防、检测、清除计算机病毒？
7. 有哪些计算机病毒的检测方法？什么是新一代的反病毒技术？
8. 有哪些反病毒软件？你会如何选择？

实践题

1. 列举两个你曾经查杀到的计算机病毒，你是如何应用反病毒软件进行查杀的，并说明如何进行手工查杀。

2. 在计算机上安装反病毒软件，说明选用此反病毒软件的原因，归纳其杀毒功能，对计算机进行杀毒处理。

3. 应用 EasyRecovery 软件查找并恢复一些你的计算机在染毒后误删除的文件。

4. 自己的手机上是否安装了反病毒软件，说明你是如何使用的。

5. 编写一个示意性的含有恶意脚本的网页，该程序可以利用死循环的原理，当浏览网页时无限制地打开新的 IE 窗口。（提示：应用 JavaScript 编写。）



网络攻防技术

学习目标

通过本章的学习,能够——

- 了解网络入侵与攻击的概念;
- 了解蜜罐技术与蜜罐网的概念;
- 知道网络攻击的主要技术;
- 知道网络攻击的防御技术;
- 知道防火墙与入侵检测技术的作用。

引导案例

如果你以为现在世界上还有任何一处可以独享清静的话,那你就错了!随着物联网的应用,各种创新的感应科技正在被应用于各种物品和设施中,令物质世界被极大程度地数据化,这意味着全球数字和有形的基础架构正在逐渐融合,事实上,几乎所有的事物——人、物体、流程、服务或组织(不管规模大小)都将被牵涉其中。

如果你以为在这样的数字化世界中,还可以轻易地找到一个百分之百的安全地带的话,那你又错了!

因为有一群"危险分子"可以轻而易举地渗透到世界上的每一个角落,他们甚至侵入白宫的核心地带,只需要几分钟!

他们并没有携带武器,但他们却开始成为世界上最危险的"恐怖分子"。不管政治、经济、军事还是其他领域,他们无孔不入。他们就是黑客,他们正在入侵!

2010 年 1 月 12 日上午,全球最大的中文搜索引擎百度遭受攻击,出现大规模无法访问的状况,范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。这次百度大面积故障时间长达五个小时,也是百度自 2006 年 9 月以来发生的最大一次严重断网事故,在国内外互联网界造成了重大影响。

2009 年 9 月,全国被恶意篡改的网站数量为 3513 个,其中政府网站(.gov.cn)被篡改的数量为 256 个;国家计算机网络应急技术处理协调中心检测到国内外被控制的僵尸网络客户端共 14 万多个,其中超过半数位于中国大陆;全国与互联网相连的网络管理中

心有95%都遭到过境内外黑客的攻击或侵入,其中银行、金融和证券机构是黑客攻击的重点。

2008年,一个全球性的黑客组织,利用欺诈程序在一夜之间从世界49个城市的银行的ATM机中盗走了900万美元。

2007年,俄罗斯黑客成功劫持Windows Update下载服务器。

2006年9月13日,百度承认遭受"大规模的不明身份黑客的攻击",导致百度搜索服务在中国各地出现了近30分钟的故障。

目前,美国因网络安全问题造成的直接经济损失每年超过170亿美元。美国金融界因计算机犯罪造成的损失每年超过100亿美元。

7.1 网络攻防技术概述

随着计算机网络技术的发展,网络的安全性和可靠性已成为不同使用层次的用户共同关心的问题。人们都希望自己的网络系统能够更加可靠地运行,不受外来入侵者干扰和破坏。但网络攻击事件频繁发生,如何防御网络攻击,保障网络安全,成为当今迫切需要解决的问题。

本节将对网络攻击的概念、网络攻击的步骤及采用的技术进行初步介绍,并列举了目前防御网络攻击的主要技术。

7.1.1 网络攻击的基本概念

1. 入侵与攻击的含义

入侵是指任何威胁和破坏系统资源的行为(如非授权或越权访问系统资源、搭线窃听信息),实施入侵行为的"人"称为入侵者。入侵的整个过程包括入侵准备、进攻与侵入。

1997年,美国国家安全通信委员会(NSTAC)下属的入侵检测小组(IDSG)给出了一个被广泛接受的入侵定义,即入侵是对信息系统的非授权访问及未经许可在信息系统中进行的操作。

攻击是入侵者实现入侵目的所采取的技术手段和方法。攻击的范围从简单的使服务器无法提供正常的服务到完全破坏、控制服务器。实施攻击行为的"人"称为攻击者。

攻击的法律定义是:攻击仅仅发生在入侵行为完全完成而且入侵者已经在目标网络内。

攻击的一般定义是指入侵者运用计算机及网络技术,利用网络的薄弱环节,侵入对方计算机及其系统进行破坏性活动,如搜集、修改、破坏和偷窃信息等。

2. 入侵与攻击的关系

入侵与攻击直接相关,入侵是目的,攻击是手段,整个入侵过程中都伴随攻击。例如在入侵者没有侵入目标之前,他想方设法利用各种手段对目标进行攻击,当攻击成功侵入目标后,入侵者利用各种手段掠夺和破坏别人的资源。

入侵者是攻击的发起人，攻击者是攻击的执行人。入侵的目的是抢占资源，但入侵者不一定有攻击能力，可能雇佣攻击者来实现入侵目的。因此，攻击是由入侵者发起并由攻击者实施的一种“非法”行为，攻击的结果就是入侵。

从网络安全角度来看，入侵与攻击没有什么本质的区别，入侵和攻击的危害是一样的。因此，有的地方入侵和攻击的概念不加区别。

3. 入侵的目标

入侵的目标主要有两类：系统和数据，所以，所对应的安全性也涉及系统安全和数据安全两个方面。

4. 入侵的途径

入侵的途径有 3 类：

(1) 物理途径，入侵者利用管理缺陷或人们的疏忽大意，乘虚而入，侵入目标主机企图登录系统或偷窃重要资源进行研究与分析；

(2) 系统途径，入侵者使用自己所拥有的较低级别的操作权限进入目标系统，复制信息、破坏资源、寻找系统漏洞以获取更高级别的操作权限等；

(3) 网络途径，入侵者通过网络渗透到目标系统中，进行破坏活动。

5. 入侵者的攻击手段

(1) 冒充：把自己伪装成别人，并以他人的名义攻击系统。

(2) 篡改：通过秘密篡改合法用户所传送的数据内容，实现自己的入侵目的。

(3) 重发：将合法用户所发出的数据修改或复制后再重发，以欺骗接收者，达到非法入侵的目的。

(4) 干扰：终止或干扰服务器为合法用户提供服务或抑制所有流向某一特定目标的数据，达到入侵的目的。

(5) 陷阱门：首先通过某种方式入侵到系统，然后安装陷阱门，并通过更改系统属性和相关特性，使入侵者在非授权情况下能对系统进行各种非法操作。

(6) 外部攻击：通过搭线窃听，截获信息，冒充系统管理人员、授权用户或系统的某个部分，设置旁路躲避鉴别与访问控制机制等入侵。

(7) 内部攻击：利用其所拥有的权限或越权对系统进行破坏活动。

(8) 特洛伊木马：利用特洛伊木马攻击不但可以拥有授权功能，还可以拥有非授权功能，一旦系统被特洛伊木马控制，整个系统将会被占领。特洛伊木马系统是具有双重功能的客户/服务体系结构。

6. 攻击的类型

(1) 按攻击目标划分。

按入侵目标划分可以分为系统型攻击与数据型攻击两类。

系统型攻击发生在网络层，破坏系统的可用性，使系统不能正常工作。通常系统型攻

击会留下明显的攻击痕迹,用户会发现系统不能工作,例如浏览器不能正常打开,邮件里出现大量不明邮件,莫名出现一些占据大量内存的进程等。

数据型攻击发生在网络的应用层,面向信息,主要目的是篡改和偷取信息。通常数据型攻击不会留下明显的痕迹,例如一些攻击者通过钓鱼网站窃取用户的个人重要信息,通过非法访问入侵企业网络或者个人计算机,从而取得个人或者企业的信息。

(2) 按攻击后果划分。

按攻击后果划分网络攻击可分为如下类型:

① 阻塞类攻击。

阻塞类攻击企图通过强制占有信道资源、网络连接资源、存储空间资源,使服务器崩溃或资源耗尽无法对外继续提供服务,但不盗窃系统资料,通常采用拒绝服务攻击或信息炸弹的方式。

拒绝服务攻击(DoS,denial of service)是典型的阻塞类攻击,它是一类个人或多人利用 Internet 协议组的某些工具,拒绝合法用户对目标系统(如服务器)和信息的合法访问的攻击。常见的方法有 TCP SYN 洪泛攻击、Land 攻击、Smurf 攻击、电子邮件炸弹等多种方式。

DoS 攻击的后果是使目标系统死机;使端口处于停顿状态;在计算机屏幕上发出杂乱信息、改变文件名称、删除关键的程序文件;扭曲系统的资源状态,使系统的处理速度降低。

② 探测类攻击。

探测类攻击主要是收集目标系统的各种与网络安全有关的信息,为下一步入侵提供帮助。主要包括扫描技术、体系结构刺探、系统信息服务收集等。目前正在发展更先进的网络无踪迹信息探测技术。

③ 控制类攻击。

控制型攻击是一类试图获得对目标计算机控制权的攻击。常见的有口令攻击、特洛伊木马与缓冲区溢出攻击。

口令截获与破解仍然是最有效的口令攻击手段,进一步的发展应该是研制功能更强的口令破解程序。

木马技术目前着重研究更新的隐藏技术和秘密信道技术。

缓冲区溢出是一种常用的攻击技术,早期利用系统软件自身存在的缓冲区溢出的缺陷进行攻击,现在研究制造缓冲区溢出。

④ 欺骗类攻击。

欺骗类攻击包括 IP 欺骗和假消息攻击,前一种通过冒充合法网络主机骗取敏感信息,后一种攻击主要是通过配制或设置一些假信息来实施欺骗攻击。主要包括 ARP 缓存虚构、DNS 高速缓存污染、伪造电子邮件等。

⑤ 破坏类攻击。

破坏类攻击指对目标计算机的各种数据与软件实施破坏的一类攻击,包括计算机病毒、逻辑炸弹等攻击手段。逻辑炸弹与计算机病毒的主要区别是逻辑炸弹没有感染能力,它不会自动传播到其他软件内。

⑥ 漏洞类攻击。

漏洞(hole)是系统硬件或者软件存在的某种缺陷,漏洞存在的直接后果是允许非法用户未经授权获得访问权或提高其访问权限。针对扫描器发现的网络系统的各种漏洞实施的相应攻击,伴随新发现的漏洞,攻击手段不断翻新,防不胜防。要找到某种平台或者某类安全漏洞也是比较简单的。在 Internet 上的许多站点,不论是公开的还是秘密的,都提供漏洞的归档和索引等。

7. 黑客的不同名字

(1) 黑客与骇客。

黑客源自英文 Hacker,一般是指计算机技术的行家,热衷于深入探究系统的奥秘,寻找系统的漏洞,为别人解决困难,并不断克服网络和计算机给人们带来的限制的人。

然而,现在(媒体报道中)通常把怀着不良的企图,强行闯入远程计算机系统或恶意干扰远程系统完整性,通过非授权的访问权限,盗取数据甚至破坏计算机系统的“入侵者”称为“黑客”,这是片面的。真正的黑客(Hacker)称这些入侵者为骇客(Cracker)或灰客。Hacker 和 Cracker 之间有着本质的不同,Hacker 发现创造东西,Cracker 专门破坏东西,所以,人们现在所说的黑客是指 Cracker。

(2) 红客。

在中国有一类黑客称为红客,他们维护国家利益,热爱自己的祖国、民族、和平,极力维护国家安全与尊严。

(3) 蓝客。

在其他国家信仰自由,提倡爱国主义的黑客们被称为蓝客,他们用自己的力量来维护网络的和平。

(4) 白客。

白客又叫安全防护者,他们使用黑客技术去做网络安全防护,通常是一些各大科技公司专门防护网络安全的人。

7.1.2 网络攻击的威胁

1. 网络攻击现状

2011 年 6 月,韩国 40 多个政府机构网站遭到黑客攻击。图 7-1 为韩国互联网振兴院的工作人员在密切监控网络系统。

除了政府机构之外,日本索尼、任天堂等游戏公司由于拥有大量在线用户群,被黑客列为首选攻击目标。索尼旗下分布在美国、希腊、泰国、印度尼西亚等地的多家子公司的网站近来陆续遭到非法入侵。黑客窃取了大量重要个人信息,包括用户姓名、住址、生日、电子邮箱、电话号码甚至信用卡账号等。据悉,涉及的用户总数可能超过 1 亿,成为索尼有史以来最大规模的信息外泄事件。日本的另一大游戏公司任天堂也于近日表示,其美国子公司运营的网站遭到非法攻击,服务器部分信息被泄露至网上。

除了跨国企业,黑客们的“黑手”也伸向了用户信息极其敏感,关乎金融安全的银行系



图 7-1　韩国互联网振兴院的工作人员在监控网络系统

统。美国花旗银行于 2011 年 6 月 8 日证实，黑客入侵了该行的网上银行客户账户，查阅或复制了大约 21 万份北美地区银行卡客户的信息。

而中国遭受攻击的次数也是居世界各国之首，近几年我国政府、部队、企业的网络频频被一些国外网络部队的黑客光顾，国家、企业重要的资料很轻易地就被窃取到，让我国损失惨重。2011 年 1—9 月中国大陆有近 3.1 万个网站被黑客篡改，其中被篡改的政府网站为 2312 个。2011 年 12 月 12 日有黑客在网上公布了中国开发者技术在线社区 CSDN 用户数据库，涉及账户密码数量达 600 万个！可以想象这些互联网企业一旦网站被黑客攻击，将会遭受惨重的损失，甚至在黑客连续的攻击下无法持续经营，破产关门。

2. 网络安全面临的威胁

互联网给社会生活带来巨大变化、给人们带来诸多便利的同时，也带来了突出的网络安全问题和社会问题，其中主要的问题有：

（1）网络黑客攻击、网络病毒等严重威胁网络运行安全；

（2）网络欺诈、网络盗窃等网络犯罪活动直接危害公共财产安全；

（3）网络淫秽色情等有害信息严重危害未成年人身心健康。

这些问题正日益引起社会各界的关注，不仅是我国，而且也成为世界各国共同面临的重大问题。

其中，人为的恶意攻击是计算机网络面临的最大威胁，敌对方的攻击和计算机犯罪都属于这一类。恶意攻击分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常使用的情况下，进行截获、窃取、破译以获得重要机密信息。

7.1.3　防御网络攻击的主要技术

网络安全已经成为各个领域必须关心的问题，其中网络攻击是威胁网络安全的最主要因素，如何采用有效的方法对网络攻击进行防御是国内外网络安全研究的重要课题。

由于网络攻击手段层出不穷，出现了许多防御网络攻击的技术。下面介绍一些有代表性的防御网络攻击技术。

1. 访问控制技术

访问控制技术是网络安全保护和防范的核心策略之一，其主要目的是确保网络资源不被非法访问和非法利用。访问控制技术所涉及的内容较为广泛，包括网络登录控制、网络使用权限控制、目录级安全控制以及属性安全控制等技术。访问控制技术主要用于对静态信息的保护，需要系统级别的支持，一般在操作系统中实现。

2. 防火墙技术

防火墙技术是用来保护内部网络免受外部网络的恶意入侵和攻击，防止计算机犯罪，将入侵者拒之门外的网络安全技术。防火墙是网络安全的屏障，是提供安全信息服务、实现网络安全的基础设施之一。它是内部网络与外部网络的边界，能够严密监视进出网络边界的数据包，能够阻挡入侵者，严格限制外部网络对内部网络的访问，也可以有效地监视内部网络对外部网络的访问。

3. 数据加密技术

数据加密能防止入侵者查看、篡改机密的数据文件，使入侵者不能轻易地查找一个系统的文件。数据加密技术是网络中最基本的安全技术，主要是通过对网络中传输的信息进行加密来保障其安全性，是一种主动的安全防御策略。

4. 入侵检测技术

入侵检测技术是网络安全技术和信息技术结合的产物，它可以实时监视网络系统的某些区域，当这些区域受到内部攻击、外部攻击和误操作时能够及时检测和立即响应，在网络系统受到危害之前拦截和响应入侵，它与静态安全防御技术（防火墙）相互配合可构成坚固的网络安全防御体系。

5. 蜜罐和密网技术

蜜罐和蜜网技术主要用于捕获和分析恶意代码及黑客攻击活动。

蜜罐的核心价值就在于对这些攻击活动进行监视、检测和分析。由于与网络隔绝并有所保护，因此闯入蜜罐计算机的入侵者无法触及网络的其他部分。通过蜜罐技术可以诱敌深入，并且不用冒着暴露网络的风险就能追踪入侵者的行为。

蜜网是在蜜罐技术上逐步发展起来的一个新的概念，又称为诱捕网络。蜜网技术实质上还是一类研究型的蜜罐技术，其主要目的仍是收集各种攻击信息。

6. 其他防御技术

除了上述主要的防御技术以外，还有一些常用的网络安全防御技术，如网络安全扫描技术、网络安全审计技术和网络安全管理技术等。

（1）网络安全扫描技术。

网络安全扫描技术是指对计算机及网络系统等设备进行相关安全检测，以查找安全隐患和可能被攻击者利用的漏洞。从安全扫描的角度来看，它既是保护计算机及网络系统必不可少的方法，也是攻击者攻击系统的技术之一。系统管理员利用安全扫描技术可以排除隐患，防止攻击者入侵；而攻击者也可以利用安全扫描技术来寻找入侵计算机及网络系统的机会。

网络安全扫描技术的原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。它既可用于对本地网络进行安全增强，也可被网络攻击者用来进行网络攻击。

安全扫描常采用基于网络的主动式策略和基于主机的被动式策略。主动式策略就是通过执行一些脚本文件模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞；而被动式策略就是对系统中不合适的设置，脆弱的口令以及其他同安全规则抵触的对象进行检查。利用被动式策略扫描称为系统安全扫描，利用主动式策略扫描称为网络安全扫描。

目前，安全扫描主要涉及四种检测技术：基于应用的检测技术、基于主机的检测技术、基于目标的漏洞检测技术、基于网络的检测技术。

（2）网络安全审计技术。

网络安全审计是在网络中模拟现实社会的监察机构，对网络系统的活动进行监视、记录并提出安全意见和建议的一种机制。利用安全审计可以有针对性地对网络运行状态和过程进行记录、跟踪和审查。通过安全审计不仅可以对网络风险进行有效评估，还可以为制定合理的安全策略和加强安全管理提供决策依据，使网络系统能够及时调整对策。

安全审计是在特定的网络环境下，为了保障网络和数据不受来自外网和内网用户的入侵和破坏，运用各种技术手段实时收集和监控网络环境中每一个组成部分的系统状态、安全事件，以便集中报警、分析、处理的一种技术手段，它是一种积极、主动的安全防御技术。

计算机网络安全审计主要包括对操作系统、数据库、Web、邮件系统、网络设备和防火墙等项目的安全审计，以及加强安全教育，增强安全责任意识。目前，网络安全审计系统主要包含以下几种功能：采集多种类型的日志数据、日志管理、日志查询、入侵检测、自动生成安全分析报告、网络状态实时监视、事件响应机制、集中管理。

（3）网络安全管理技术。

网络安全管理是指为实现网络安全的目标而采取的一系列管理制度和技术手段，包括安全检测、监控、响应和调整的全部控制过程。需要指出的是，不论多么先进的网络安全技术，都只是实现网络安全管理的手段，网络安全重要的是有效地管理，要使先进的网络安全技术发挥较好的效果，就必须建立良好的网络安全管理体制，制定切合实际的网络安全管理制度，加强网络安全的规范化管理力度，强化网络管理人员和使用人员的安全防范意识。只有网络管理人员与使用人员共同努力，才能有效地防御网络入侵和攻击，才能使网络安全得到保障。

网络安全是一项复杂的系统工程，防御网络入侵与攻击只是保障网络信息安全的一

部分。随着计算机网络的快速应用和普及,网络安全的不确定因素也越来越多,必须综合考虑各种安全因素,认真分析各种可能的入侵和攻击形式,采取有效的技术措施,制定合理的网络安全策略和配套的管理办法,防止各种可能的入侵和攻击行为,避免因入侵和攻击造成的各种损失。

7.2 网络攻击的手段与工具

本节主要介绍网络攻击模型,以及网络攻击常见的手段与工具。

7.2.1 网络攻击行为模型

入侵者攻击一个系统的最终目标一般是获得目标系统的管理员权限,对目标系统进行绝对控制,窃取其中的机密文件等重要信息。一般情况下,网络攻击通常遵循一种行为模型,包含侦查、攻击与侵入、退出三个阶段,如图 7-2 所示。

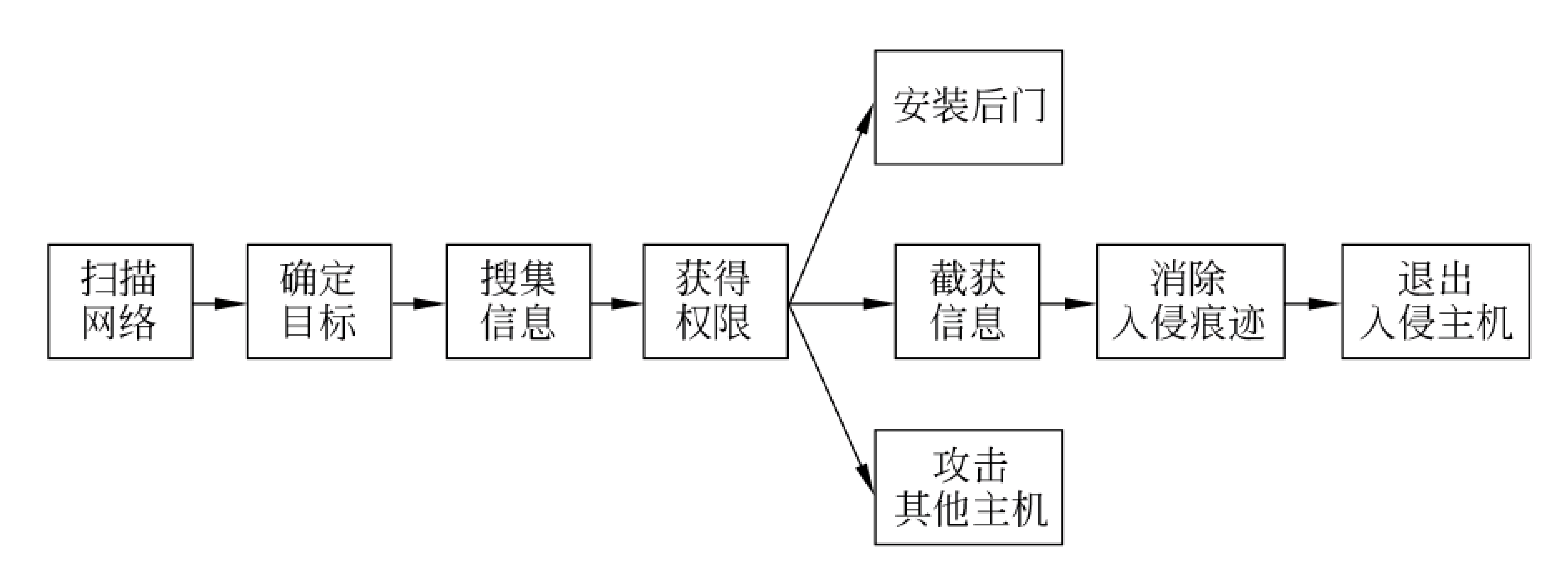


图 7-2 网络攻击行为模型

1. 侦查

侦查阶段攻击者需要在发动攻击前了解目标的网络结构,搜集各种目标系统的信息等。主要包含以下步骤:

(1) 扫描网络(隐藏地址):攻击者首先扫描网络,寻找可以利用的别人的计算机当“傀儡机”,以隐藏自己真实的 IP 地址等位置信息。

(2) 确定目标:网络上有许多主机,攻击者接下来的工作就是寻找并确定目标主机。

(3) 搜集信息:确定要攻击的目标后,攻击者就会设法收集其所在的网络结构信息,包括网关路由、防火墙、入侵检测系统(IDS)等,最简单的就是用 tracert 命令追踪路由,也可以发一些数据包看其是否能通过来猜测防火墙过滤规则的设定等。了解了网络结构信息之后,攻击者还会对主机进行全面的系统分析,以寻求该主机的操作系统类型、所提供服务及其安全漏洞或安全弱点,攻击者可以使用一些扫描器工具,轻松获取目标主机运行的操作系统及版本,系统里的账户信息,WWW、FTP、Telnet、SMTP 等服务器程序是何种版本和服务类型,端口开放情况等资料,主要方法有端口扫描、服务分析、协议分析和用户密码探测等。

总之,攻击者在锁定目标后首先要搜集目标的网络结构信息与系统信息。

2. 攻击与侵入

当入侵者通过侦查收集到足够的信息后，对系统的安全弱点有了充分了解后就会发动攻击。攻击与侵入阶段主要包含以下步骤：

(1) 获得权限：入侵者利用找到的安全漏洞或弱点，获取未授权的访问权限，例如利用缓冲区溢出或蛮力攻击破解口令，然后登录系统。然后再利用目标系统的操作系统或应用程序的漏洞，试图提升在该系统上的权限，获得管理员权限，侵入系统。

(2) 安装后门：获得控制权后，入侵者为了能长时间保留和巩固他对系统的控制权，确保以后能够重新进入系统，会留下后门为以后实施攻击提供方便，他们会更改某些系统设置、在系统中植入特洛伊木马或其他一些远程控制程序。

(3) 截获信息：留下后门后，入侵者可能会窃取主机上的软件资料、客户名单、财务报表、信用卡号等各种敏感信息，也可能什么都不做，只是把该系统作为他存放黑客程序或资料的仓库，也可能会利用这台已经攻陷的主机去继续他下一步的攻击，比如继续入侵内部网络，或者将这台主机作为 DDoS(distributed denial of service，分布式拒绝服务)攻击的一员。

3. 退出

一般入侵成功后，入侵者为了不被管理员发现，会把入侵痕迹清除干净，清除日志、删除复制的文件，隐藏自己的踪迹。日志往往会记录一些入侵攻击的蛛丝马迹，入侵者会删除或修改系统和应用程序日志中的数据，或者用假日志覆盖它。

7.2.2 网络攻击手段

网络攻击常用的手段包括网络监听、ARP 欺骗、缓冲区溢出和拒绝服务等。

1. 网络监听

黑客也会利用网络监听技术对其他用户进行攻击，黑客可以利用网络监听来截取主机口令，当黑客控制一台主机之后，如果他想通过这台主机控制其所在的整个局域网，网络监听往往是他们的最佳选择。

网络监听基本原理：在以太网中，数据包是发送给源主机连接在一起的所有主机，包中包含着应该接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才接收，其他主机则丢弃。但是，当主机工作在监听模式(混杂模式)下，就可以监听并记录下同一网段上所有的数据包，无论数据包中的目标地址是什么。攻击者可以从数据包中提取机密或敏感的数据信息，如登录名、口令等。

2. IP 电子欺骗

IP 电子欺骗(IP spoofing)也叫做 IP 地址伪造(IP address forgery)或主机文件劫持(host file hijack)，黑客用这种劫持技术伪装成主人来掩饰身份、进行网站诈骗、劫持浏览器或获得网络访问权限。它的工作的方式是：劫持者得到合法主机的 IP 地址并更改包

头，所以合法网站看上去就像源头了。

当 IP 电子欺骗用在劫持浏览器时，用户在合法网站输入 URL，就会被劫持者带入一个伪造网页。例如，如果劫持者伪造了国会网站的库，任何输入 www.loc.gov 这个 URL 的互联网用户都会看到劫持者创造的仿造内容。

如果用户在伪造网页上与动态内容互动，劫持者就能获得敏感信息、计算机或网络资源的访问权。他能盗取或更改敏感数据，如信用卡号或密码，或者安装流氓插件。劫持者还能控制被盗取的计算机，把它作为僵尸网络的一部分来发送垃圾邮件。

3. ARP 欺骗

在局域网中，通信前必须通过 ARP 协议（地址解析协议：将域名翻译成对应的 32 位 IP 地址的协议）来完成 IP 地址转换为第二层物理地址（即 MAC 地址）。ARP 协议对网络安全具有重要的意义。ARP 欺骗攻击是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的攻击技术。

ARP 欺骗攻击基本原理：网内的任何一台计算机都可以轻松地发送 ARP 广播，来宣称自己的 IP 和自己的 MAC。这样收到的计算机都会在自己的 ARP 表格中建立一个它的 ARP 项，记录它的 IP 和 MAC 地址。即使这个广播是错误的其他计算机也会接受。例如：192.168.1.11 计算机 MAC 是 00:00:00:11:11:11，它使用 ARP 欺骗，在内网广播自己的 IP 地址是 192.168.1.254（其实是路由器的 IP），MAC 地址是 00:00:00:11:11:11（它自己的真实 MAC）。这样大家会把给 192.168.1.254 的信息都发给 00:00:00:11:11:11，也就是 192.168.1.11。用这个方法欺骗者只需要做一个软件，就可以在内网欺骗所有上网的计算机。而内网所有收到他发来信息的计算机都会把它误认为内网的网关。所有上网信息都会通过他的 MAC 地址发给这个计算机，由于找不到真正的网关，这些被骗的计算机就无法上网。而发送的所有信息都会被这个盗号计算机收到，通过分析收到的信息他可以在里面找到有用的信息，特别是有关于账号的部分。

4. 缓冲区溢出

缓冲区溢出攻击技术是利用缓冲区溢出漏洞所进行的攻击行动。缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统关机、重新启动等后果。

缓冲区溢出攻击原理：缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上。理想的情况是：程序会检查数据长度，而且并不允许输入超过缓冲区长度的字符。但是绝大多数程序都会假设数据长度总是与所分配的储存空间相匹配，这就为缓冲区溢出埋下隐患。操作系统所使用的缓冲区，又被称为“堆栈”，在各个操作进程之间，指令会被临时储存在堆栈当中，堆栈也会出现缓冲区溢出。

通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。例如下面的程序：

```
void function(char * str) {
char buffer[16]; strcpy(buffer,str);
}
```

其中的 strcpy()函数将直接把 str 中的内容复制到 buffer 中。这样只要 str 的长度大于 16,就会造成 buffer 的溢出,使程序运行出错。

5. DoS 与 DDoS 攻击

(1) DoS 拒绝服务。

DoS(denial of service,拒绝服务)攻击是通过利用主机特定漏洞进行攻击导致网络失效、系统崩溃、主机死机而无法提供正常的网络服务功能,造成拒绝服务,或者利用合理的服务请求来占用过多的服务器资源(包括网络宽带、文件系统空间容量或者网络连接等),致使服务器超载,最终无法响应其他用户正常的服务请求。

DoS 攻击一般采用一对一的方式。

常见的 DoS 攻击方式有死亡之 ping(ping of death)、TCP 全连接攻击、SYN Flood、SYN/ACK Flood、TearDrop、Land、Smurf、刷 Script 脚本攻击、UDP 攻击等。

(2) DDoS 分布式拒绝服务。

DDoS 攻击又称“洪水式攻击”,是在 DoS 攻击的基础上产生的一种分布式、协作式的大规模拒绝服务攻击方式,其攻击策略侧重于通过很多“僵尸主机”(被攻击者入侵过或可间接利用的主机)向受害主机发送大量看似合法的网络数据包,从而造成网络阻塞或服务器资源耗尽而导致拒绝服务,分布式拒绝服务攻击一旦实施,攻击网络数据包就会如洪水般涌向受害主机,从而把合法用户的网络数据包淹没,导致合法用户无法正常访问服务器的网络资源。

DDoS 攻击是目前难以防范的攻击手段,这种攻击主要针对大的站点。由于攻守双方系统资源的差距悬殊,DDoS 攻击具有更大的破坏性。

DDoS 攻击的形式主要有流量攻击和资源耗尽攻击。前者主要是针对网络带宽的攻击,即大量攻击包导致网络带宽被阻塞,合法网络包被虚假的攻击包淹没而无法到达主机。后者主要是针对服务器主机的攻击,即通过大量攻击包导致主机的内存被耗尽或 CPU 被占完而导致无法提供正常网络服务。

DDoS 攻击采用多对一的方式。

常见的 DDos 攻击方式有 SYN Flood、ACK Flood、UDP Flood、ICMP Flood、TCP Flood、Script Flood 等。

7.2.3 网络攻击工具

所谓网络攻击工具是指编写出来用于网络攻击方面的工具软件,用来执行一些诸如扫描端口、黑客程序入侵、监测系统等功能,大部分是以恶意攻击为目的的攻击性软件,常见的有木马程序、病毒程序、炸弹程序等,另外还有一部分软件是为了破解某些软件或系统的密码而编写的,一般也出于非正当的目的。了解这些工具可以了解网络的攻击手段,从而更好地防御网络攻击。

1. 木马程序

一般的木马都有客户端和服务器端两个执行程序,其中客户端是用于黑客远程控制植入木马的计算机的程序,服务器端程序即木马程序。如果攻击者要通过木马入侵系统,第一步就是要让木马的服务器端程序在目标计算机中运行。一旦运行成功,木马程序就可以获得系统管理员的权限,在用户毫无觉察的情况下,对计算机做任何能做的事情。

常见的木马程序类软件包括冰河、蓝色火焰和灰鸽子等。

2. 扫描工具

扫描工具能够自动检测远程或本地主机安全弱点的程序,通过它可以获得远程计算机的各种端口分配及提供的服务和它们的版本。扫描器工作时是通过选用不同的 TCP/IP 端口的服务,并记录目标主机给予的应答,以此搜集到关于目标主机的各种有用信息的。

常见的扫描工具类软件有流光、X-way2.5、Superscan 等软件。流光是国内最著名的扫描、入侵工具,集端口扫描、字典工具、入侵工具、口令猜解等多种功能于一身,界面豪华,功能强大。它可以探测 POP3、FTP、SMTP、IMAP、SQL、IPC、IIS、FINGER 等各种漏洞,并针对各种漏洞设计了不同的破解方案,能够在有漏洞的系统上轻易得到被探测的用户密码。它的界面如图 7-3 所示。

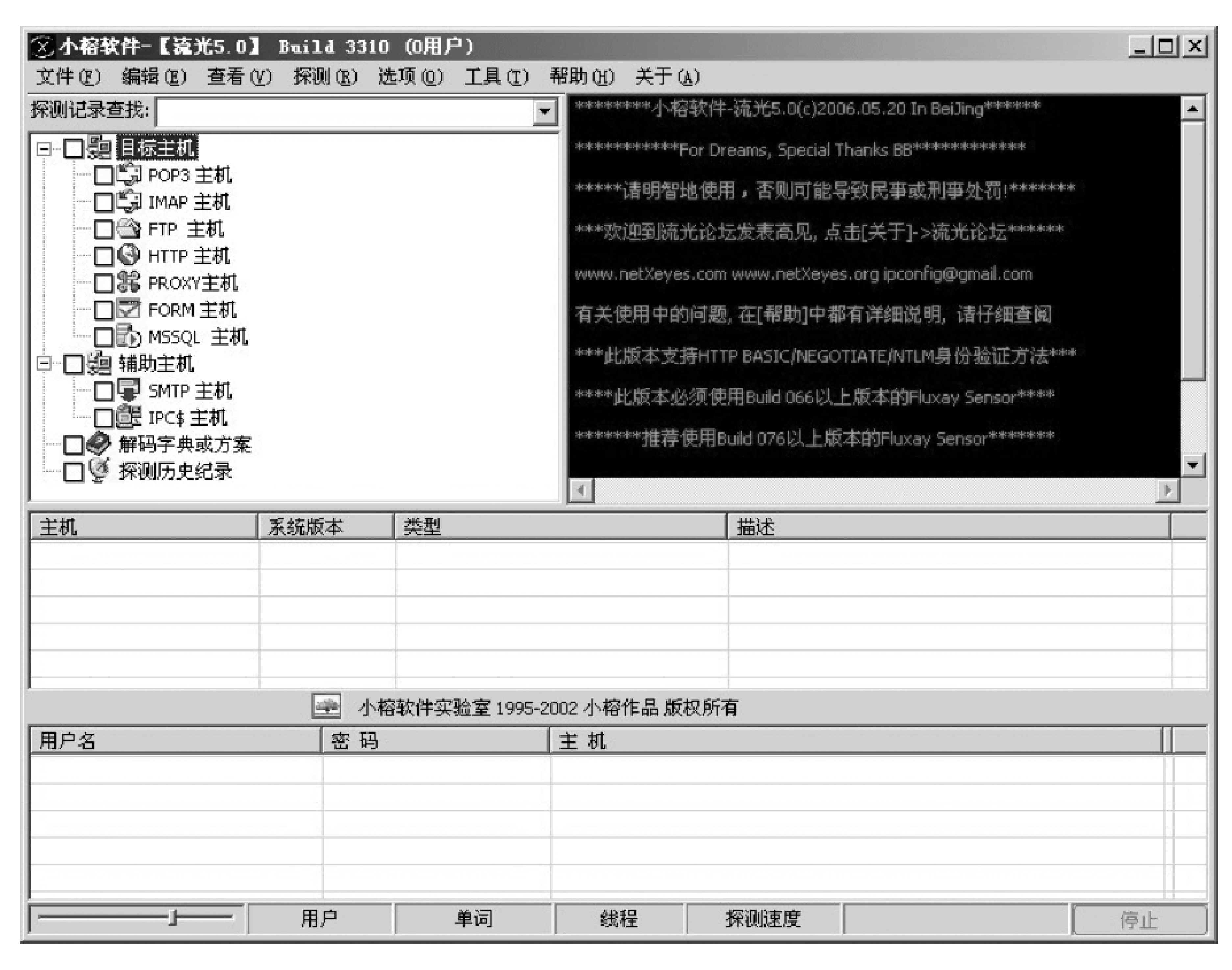


图 7-3 流光软件的主界面

3. 破解工具

利用破解工具可以检查密码的安全性及找回忘记的密码,但用心不良的人也可以用

它来破解他人的密码,以达自己不可告人的目的。

根据破解原理的不同,破解工具大致可分为穷举法破解器和查看法破解器两种。穷举法,又叫暴力破解法,其过程是从字典文件里抽出一个字段来和要破解的密码进行对比,直到破解出密码或字典里的字段全部试完为止。这种守株待兔的方法看似简单,但由于黑客字典通常包含了很多黑客经验的累积,所以此法对于安全意识不强的用户,破解率是很高的。查看法是指程序通过嗅探系统漏洞来获得密码文件的方法。

常用的破解工具有溯雪密码探测工具、网络刺客Ⅱ、黑雨等。大部分破解软件都能通过嗅探系统漏洞来获得信息。例如网络监听工具 Sniffer,中文翻译为嗅探器,它是利用计算机网络接口截获数据报文的一种工具。它工作在网络的底层,能把网络传输的全部数据记录下来。它实际上是一种网络管理工具,主要功能有分析网络协议、定位网络故障;帮助网络管理员查找网络漏洞和检测网络性能;分析网络的流量,找出所关心的网络中潜在的问题;收集有用的数据,这些数据可以是用户的账号和密码,也可以是一些商用机密数据等。图 7-4 是 SnifferPro 的主界面。

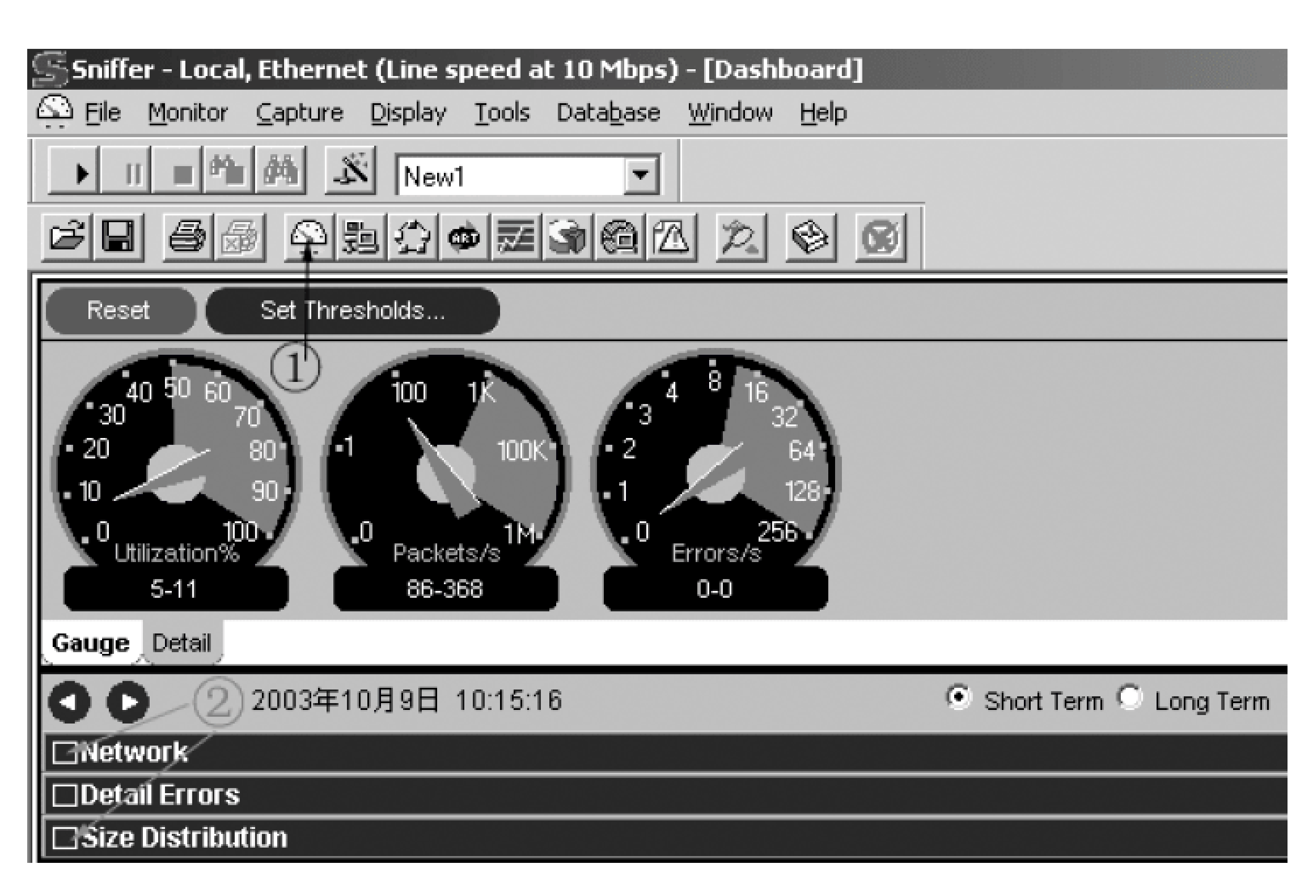


图 7-4　SnifferPro 的主界面

4. 炸弹工具

炸弹攻击的基本原理是利用特殊工具软件,在短时间内向目标机集中发送大量超出系统接收范围的信息或者垃圾信息,目的在于使对方目标机出现超负荷、网络堵塞等状况,从而造成目标的系统崩溃及拒绝服务。常见的炸弹有邮件炸弹、逻辑炸弹、聊天室炸弹等。

7.3　防御网络攻击的几种技术

在网络环境下,网络被攻击是难免的。但是,通过加强管理和采用必要的技术手段可以减少入侵和攻击行为,避免因入侵和攻击造成的各种损失。

本节主要介绍网络攻击的防御策略和针对一些常见的攻击的防御方法。

7.3.1 防御网络攻击的策略

从实际情况看，没有人能绝对保证计算机不受黑客的攻击，但可以采取一些预防性措施将黑客危害降到最低程度。下面介绍一些日常中的积极防御策略。

1. 提高安全意识

不要随意打开来历不明的电子邮件及文件，不要随便运行不太了解的人给你的程序，例如“特洛伊”类黑客程序就是骗你运行。

密码设置尽可能使用字母数字混排，单纯的英文或者数字很容易穷举，将常用的密码设置不同，防止被人查出一个，连带到重要密码，而且重要密码最好定期更换。

不随便运行黑客程序，许多这类程序运行时会发出用户的个人信息。最后及时下载安装系统补丁程序，更新系统。

最好不要浏览一些不知名的网站，特别是一些病毒类和黑客类网站，有些网站在介绍防病毒和黑客技术的同时，也会将病毒和木马等放到访问者的计算机上。如果要下载软件，应在安装该软件前要先用杀毒软件清除病毒和木马。

2. 积极采取防范措施

(1) 安装防病毒和防火墙软件并及时更新病毒库。

应该在计算机上安装实时防病毒软件，如诺顿、江民、瑞星、金山毒霸等，用户至少每周在线升级一次杀毒软件，这样才能使防病毒软件最有效。当刚安装完一个新系统后，就要及时安装防病毒软件，并至少每星期更新一次病毒库。

如果用户使用因特网，特别是使用宽带，就非常有必要使用防火墙软件来保护自己的隐私，防止不速之客访问用户系统。如果用户的系统没有加设有效防护，那么个人信息、信用卡号码和其他密码都有可能被窃取。要及时、正确配置防火墙参数，才能达到防御黑客攻击的目的。

(2) 安装入侵检测软件。

安装入侵检测软件可以极大地帮助网络管理员监控可疑数据流，因为系统日志对安全事件的记录很不全面，但如果有入侵检测软件的帮助，就可以定位问题的所在。

(3) 及时更新操作系统。

由于操作系统和网络协议等自身的不完善性和缺陷，使计算机病毒和黑客有机可乘。许多黑客都是利用已知的操作系统漏洞进行攻击的。例如，世界著名的微软公司几乎每周都要发布操作系统漏洞补丁程序。如果能及时、提前升级自己的操作系统，主动给操作系统和网络系统打上“补丁”，就会避免很多攻击，减少攻击带来的破坏。

(4) 经常系统备份。

经常进行系统备份能够有效降低一些病毒或黑客的损害程度。包括用户数据的备份、软件配置文件的备份等。出现问题后不要忙于恢复，先确定问题所在，解决后再恢复系统，这样可以避免问题的进一步扩大，否则在做恢复工作时可能出现破坏原有备份数据的危险。

3. 访问控制策略

访问控制是网络安全防范和保护的主要策略,也是维护网络系统安全、保护网络资源的重要手段,其主要任务是保证网络资源不被非法使用和非法访问。各种安全策略必须相互配合才能真正起到保护作用,但访问控制可以说是保证网络安全的最重要的核心策略之一。

4. 数据加密策略

加密技术是网络安全最有效的技术之一。通过对网内数据、文件、口令和控制信息进行加密从而达到保护网上传输的数据的目的。加密的网络不但可以防止非授权用户的窃听和入网,而且也可以有效防止恶意软件攻击。

5. 网络安全管理策略

想要建立一个安全的网络环境就需要严格的管理,正所谓:"三分技术,七分管理"。在网络安全中,除了采用技术措施之外,加强网络的安全管理,制定有关规章制度,对于确保网络的安全、可靠地运行,将起到十分关键的作用。网络的安全管理策略包括:确定安全管理等级和安全管理范围;制定有关网络操作实验规程和人员管理制度;制定网络系统的维护制度和应急措施等。

7.3.2 防御网络攻击的方法

除了防御策略,还可以采用如下防御方法防止网络攻击和入侵。

1. 防范端口扫描

关闭闲置和有潜在危险的端口。除正常使用的计算机端口外(如访问网页需要的HTTP80端口,QQ的4000端口等不能被关闭),将所有其他端口都关闭。因为对黑客而言,所有的端口都可能成为攻击的目标。

在以Windows NT为核心的操作系统(如Windows 2003/XP/7)中要关闭掉一些闲置端口是比较方便的,可以采用"定向关闭指定服务的端口"和"只开放允许端口的方式"。计算机的一些网络服务会由系统分配默认的端口,将一些闲置的服务关掉,其对应的端口也会被关闭。进入"控制面板"中的"管理工具"下的"服务"项内,关闭掉计算机中一些没有使用的服务(如FTP服务、DNS服务、IISAdmin服务等),同时该服务对应的端口也就被停用了。至于"只开放允许端口的方式"可以利用系统的"TCP/IP筛选"功能实现,设置的时候,"只允许"系统中一些基本网络通信需要的端口即可。

2. 防范Sniffer

Sniffer嗅探程序最大的危险性就是很难被发现。因为嗅探程序是一种被动的接收程序,属于被动触发的,它只会接收数据包,而不发送任何数据。尽管如此,嗅探程序还是会产生一些数据流,根据计算机是否存在以下现象,嗅探程序有时候也能够被检测出来。

(1) 网络通信掉包率反常地高。

通过一些网络软件,可以看到信息包传送情况,像 ping 这样的命令会显示掉了百分之几的包。如果网络中有人在监听,那么信息包传送将无法每次都顺畅地流到目的地(这是由于 Sniffer 拦截每个包导致的)。

(2) 网络带宽出现反常。

通过某些带宽控制器(通常是防火墙所带),可以实时看到目前网络带宽的分布情况,如果某台计算机长时间占用了较大的带宽,这台计算机就有可能在监听。在非高速信道上,如 56Kddn 等,如果网络中存在 Sniffer,用户就可以察觉出网络通信速度的变化。

(3) 查看计算机上当前正在运行的所有程序。

查看正在运行的所有程序的操作通常并不可靠,但可以控制计算机中程序运行。在 UNIX 系统下使用下面的命令:ps -aux 或 ps -augx。这个命令列出当前的所有进程、启动这些进程的用户、它们占用 CPU 的时间、占用内存的多少等。

在 Windows 系统下,按下 Ctrl+Alt+Del 组合键,看一下任务列表。不过,编程技巧高的 Sniffer 即使正在运行,也不会出现在这里的。

(4) 在系统中搜索,查找可疑的文件。但入侵者可能使用自己编写的程序,所以都会给发现 Sniffer 造成相当大的困难。

除此之外还有许多工具,能用来查看系统是否在混杂模式。从而发现是否有一个 Sniffer 正在运行。

3. 防范 IP 电子欺骗

IP 电子欺骗如果被一个有恶意的攻击者入侵成功,则危害巨大。虽然从技术上该手段是复杂的,但并不是不能防止,所以,根据前面所述 IP 电子欺骗的特点,提出如下综合预防策略:

(1) 站点管理人员要有足够的安全意识,提高警惕,不要轻易相信自己的系统安全已经是万无一失。特别对于一些重要的商业或政府网站,对于自己信任的主机,要经常交换信息,如果信任的主机在某一段时间正受到攻击(如拒绝服务式攻击),要提高本主机的安全等级,必要时和信任主机的管理人员用电话或电子邮件联系进行确认。

(2) 在网络设计时,应多采用一些技术手段提高站点安全,如使用路由器和防火墙等设备。

(3) 严密监视网络,识别那些声称源于本地网络的包。有几类包可被监视到。最基本的是那些源地址和目的地址的网络部分相同但又不是本地网络的 TCP 包。

(4) 诱惑入侵者。即使再好的网络设备也可能被入侵者欺骗,网络管理员可在本机上预先设置好“诱饵”,如“密码,机密”等字眼的文件,并将这些文件与专用的警报系统连接,一旦入侵者触动机关,网络管理人员可对入侵者进行实时跟踪。

4. 防范 ARP 欺骗

(1) 不要把网络安全信任关系建立在 IP 地址的基础上或硬件 MAC 地址基础上(RARP 同样存在欺骗的问题),较为理想的信任关系应该建立在 IP+MAC 基础上。即

在地址栏使用 IP 地址和 MAC 地址。

(2) 在本机和网关设置静态的 MAC-IP 对应表,不要让主机刷新已设定好的转换表。在三层交换机上设定静态 ARP 表。

(3) 除非很有必要,否则停止使用 ARP,将 ARP 作为永久条目保存在对应表中。在 Linux 下用 ifconfig-arp 可以使网卡驱动程序停止使用 ARP。

(4) 在本机地址使用 ARP,发送外出的通信使用代理网关。

(5) 修改系统拒收 ICMP 重定向报文,在 Linux 下可以通过在防火墙上拒绝 ICMP 重定向报文或者是修改内核选项重新编译内核来拒绝接收 ICMP 重定向报文。在 Windows 2000 下可以通过防火墙和 IP 策略拒绝接收 ICMP 报文。

5. 防范 DDoS 攻击

由于攻击具有隐蔽性,到目前为止还没有找到对 DDoS 攻击行之有效的解决方法。因此只能加强安全防范意识,以预防为主。

(1) 定期扫描。

要定期扫描现有的网络主节点,清查可能存在的安全漏洞,对新出现的漏洞及时进行清理。骨干节点的计算机因为具有较高的带宽,是黑客利用的最佳位置,因此对这些主机本身加强主机安全是非常重要的。而且连接到网络主节点的都是服务器级别的计算机,所以定期扫描漏洞就变得更加重要了。

(2) 在骨干节点配置防火墙。

防火墙本身能抵御 DDoS 攻击和其他一些攻击。在发现受到攻击的时候,可以将攻击导向一些牺牲主机,这样可以保护真正的主机不被攻击。当然导向的这些牺牲主机可以选择不重要的,或者是 Linux 以及 UNIX 等漏洞少和天生防范攻击优秀的系统。

(3) 用足够的计算机承受黑客攻击。

这是一种较为理想的应对策略。如果用户拥有足够的容量和足够的资源给黑客攻击,在它不断访问用户、夺取用户资源之时,自己的能量也在逐渐耗失,或许未等用户被攻死,黑客已无力支招儿了。不过此方法需要投入的资金比较多,平时大多数设备处于空闲状态,和目前中小企业网络实际运行情况不相符。

(4) 充分利用网络设备保护网络资源。

所谓网络设备是指路由器、防火墙等负载均衡设备,它们可将网络有效地保护起来。当网络被攻击时最先死掉的是路由器,但其他计算机没有死。死掉的路由器经重启后会恢复正常,而且启动起来还很快,没有什么损失。若其他服务器死掉,其中的数据会丢失,而且重启服务器又是一个漫长的过程。特别是一个公司使用了负载均衡设备,这样当一台路由器被攻击死机时,另一台将马上工作,从而最大程度地削减了 DDoS 的攻击。

(5) 过滤不必要的服务和端口。

可以使用 Inexpress、Express、Forwarding 等工具来过滤不必要的服务和端口,即在路由器上过滤假 IP。例如 Cisco 公司的 CEF(cisco express forwarding)可以针对封包 Source IP 和 Routing Table 做比较,并加以过滤。只开放服务端口成为目前很多服务器的流行做法,例如 WWW 服务器只开放 80 而将其他所有端口关闭或在防火墙上做阻止策略。

(6) 检查访问者的来源。

使用 Unicast Reverse Path Forwarding 等通过反向路由器查询的方法检查访问者的 IP 地址是否是真的,如果是假的,它将予以屏蔽。许多黑客攻击常采用假 IP 地址方式迷惑用户,很难查出它来自何处。因此,利用 Unicast Reverse Path Forwarding 可减少假 IP 地址的出现,有助于提高网络安全性。

(7) 过滤所有 RFC1918 IP 地址。

RFC1918 IP 地址是内部网的 IP 地址,像 10.0.0.0、192.168.0.0 和 172.16.0.0,它们不是某个网段的固定的 IP 地址,而是 Internet 内部保留的区域性 IP 地址,应该把它们过滤掉。此方法并不是过滤内部员工的访问,而是将攻击时伪造的大量虚假内部 IP 过滤,这样也可以减轻 DDoS 的攻击。

(8) 限制 SYN/ICMP 流量。

用户应在路由器上配置 SYN/ICMP 的最大流量来限制 SYN/ICMP 封包所能占有的最高频宽,这样,当出现大量的超过所限定的 SYN/ICMP 流量时,说明不是正常的网络访问,而是有黑客入侵。早期通过限制 SYN/ICMP 流量是最好的防范 DoS 的方法,虽然目前该方法对于 DDoS 效果不太明显了,不过仍然能够起到一定的作用。

7.4 防火墙技术

古人在建筑物的两侧山墙和后檐墙上,不开门窗,不采用可燃材料,谓之风火檐,也称封火檐。这是防火墙的一种形式。这里所谈的防火墙并不是真正用来防火的墙,而是一种网络安全技术。如现在国内计算机用户普遍安装的 360 安全卫士中的 360 木马防火墙,就是一款基础的个人用户防火墙产品。它的界面如图 7-5 所示。

本节主要介绍防火墙的含义、分类、功能与产品。

7.4.1 防火墙的含义

当一个用户计算机或内联网络连接到外联网络后,它就可以通过外联网络访问其他主机或网络并与之通信。同时,外界的主机也可以访问到这台联网主机或内联网络。而内联网络的资源系统恰恰是违法者垂涎的宝藏,内联网络经常需要面对因此产生的各种恶意行为。首先是非法的信息获取,即黑客、入侵者或者闯入者试图偷走敏感信息,以及试图盗窃数据、表格、磁盘空间和 CPU 资源等对象的行为。其次是有意或者无意的内部雇员非授权的数据使用。再次是通过路由器、主机或者服务器蓄意破坏文件系统或者阻止授权用户的网络访问服务。

为了安全起见,需要在本地计算机或内联网络与外联网络之间设置一道屏障,这道屏障能够保护本地计算机或内联网络免遭来自外联网络的威胁和入侵。这道屏障就叫做防火墙。严格地说,防火墙技术指的是目前最主要的一种网络防护技术,而采用该技术的网络安全系统叫做防火墙系统,包括硬件设备、相关的软件代码和安全策略。在这里统一地称其为防火墙。防火墙是技术与设备的集成系统,而并非单指某一个特定的设备或软件。

防火墙系统如图 7-6 所示。



图 7-5　360 木马防火墙

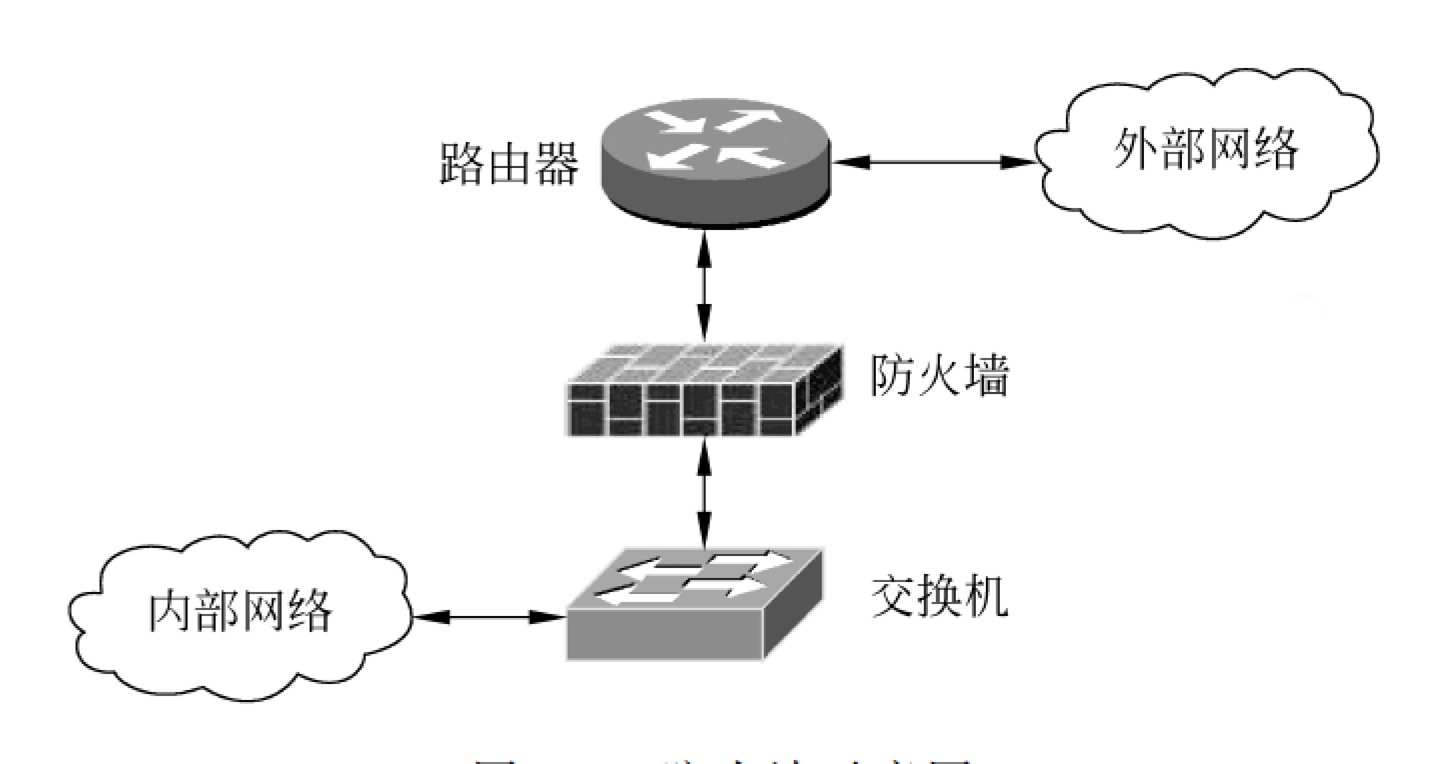


图 7-6　防火墙示意图

7.4.2　防火墙的分类

防火墙根据参照标准的不同有多种分类方式，下面主要介绍按技术划分和按具体实现划分的防火墙。

1. 按防火墙采用的主要技术划分

(1) 包过滤型防火墙。

包过滤型防火墙工作在 ISO 7 层模型的传输层以下，根据数据包头部各个字段进行过滤，包括源地址、端口号以及协议类型等。

包过滤方式不针对具体的网络服务而是针对数据包本身进行过滤，适用于所有网络服务。目前大多数的路由器设备都集成了数据包过滤的功能，具有很高的性价比。但是包过滤方式也有明显的缺点：过滤判别条件有限，安全性不高；过滤规则数目的增加会极

大地影响防火墙的性能；很难进行对用户身份进行验证；对安全管理人员素质要求高等。

(2) 代理型防火墙。

代理型防火墙工作在 ISO 7 层模型的最高层——应用层。它完全阻断了网络访问的数据流：它为每一种服务都建立了一个代理，内部网络与外部网络之间没有直接的服务连接，都必须通过相应的代理审核后再转发。

2. 按防火墙的具体实现划分

(1) 多重宿主主机。

多重宿主主机是放在内网与外网接口上的一台堡垒主机。它最少有两个网络接口：一个与内网相连，另外一个与外网相连。内、外网之间禁止直接通信，需通过多重宿主主机上应用层数据共享或者应用层代理服务来完成。

(2) 屏蔽主机。

这种防火墙由内部网络和外部网络之间的一台过滤路由器和一台堡垒主机构成。它强迫所有外部主机与堡垒主机相连接，而不让它们与内部主机直接相连。为了达到这个目的，过滤路由器将所有的外部到内部的连接都路由到了堡垒主机上，让外部网络对内部网络的访问通过堡垒主机上提供的相应代理服务器进行。对于内部网络到外部不可信网络的出站连接则可以采用不同的策略：有些服务可以允许绕过堡垒主机，直接通过过滤路由器进行连接；其他的一些服务则必须经过堡垒主机上的运行该服务的代理服务器实现。

(3) 屏蔽子网。

屏蔽子网与屏蔽主机在本质上是一样的，它对网络的安全保护通过两台包过滤路由器和在这两台路由器之间构筑的子网，即非军事区来实现。在非军事区里放置堡垒主机，还可能有公用信息服务器。

与外部网络相连的过滤路由器只允许外部系统访问非军事区内的堡垒主机或者公用信息服务器。与内部网络相连接的过滤路由器只接收从堡垒主机来的数据包。内部网络与外部网络的直接访问是被严格禁止的。

(4) 其他实现结构的防火墙。

其他结构的防火墙系统都是上述几种结构的变形，主要有：一个堡垒主机和一个非军事区、两个堡垒主机和两个非军事区、两个堡垒主机和一个非军事区等，目的都是通过设定过滤和代理的层次使得检测层次增多从而增加安全性。

此外，按受保护的对象可以将防火墙划分为单机防火墙和网络防火墙；按使用者可划分为企业级防火墙和个人防火墙，个人防火墙实际上与单机防火墙是一种，只是看待问题出发点不同；按形式则可以划分成软件防火墙、独立硬件防火墙和模块化防火墙，个人防火墙一般都是软件防火墙，而对于有自己办公网络的企业，通常要在内网和外网之间配置硬件防火墙，模块化防火墙则是在路由器中集成了防火墙的功能。

7.4.3 防火墙的功能

1. 防火墙是网络安全的屏障

一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤

不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络,这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击,如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置,能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比,防火墙的集中安全管理更经济。例如在网络访问时,一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上,而集中在防火墙一身上。

3. 对网络存取和访问进行监控审计

如果所有的访问都经过防火墙,那么,防火墙就能记下这些访问并作出日志记录,同时也能提供网络使用情况的统计数据。当发生可疑动作时,防火墙能进行适当的报警,并提供网络是否受到监测和攻击的详细信息。另外,收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击,并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分,可实现内部网重点网段的隔离,从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者,隐私是内部网络非常关心的问题,一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣,甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透露内部细节的如 Finger、DNS 等服务。Finger 显示了主机的所有用户的注册名、真名、最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度,这个系统是否有用户正在连线上网,这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的 DNS 信息,这样一台主机的域名和 IP 地址就不会被外界所了解。

7.4.4 常用的防火墙产品

1. 常用的硬件防火墙产品

硬件防火墙是指设置在不同网络结构之间的一种硬件设备,它是不同网络或网络安全域之间信息的唯一出入口。通过监测、限制、更改跨越防火墙的数据流,可以尽可能地对外部屏蔽网络内部的信息、结构和运行状况;可以控制对服务器与外部网络的访问等,从而达到安全防范的作用。由于防火墙的生产厂商数量众多,所以下面只选取几个具有

代表性的厂商的防火墙产品进行简要介绍。

(1) 瞻博网络 Juniper。

Juniper由三位留美的清华学子创建,其防火墙和VPN产品无论从性能指标还是质量上都位居世界前列。Juniper/NetScreen出品的NetScreen系列防火墙是由硬件来实现防火墙技术的网络安全产品。它将NAT、包过滤、DMZ、VPN、负载均衡及流量控制等技术集成在同一设备里,具有速度快、功能完善、设置简单和高性能价格比的优点。

其具体功能特性为:拥有专用的操作系统ScreenOS,拥有专门优化的硬件增强技术,集成VPN,灵活的流量管理,基于ASIC的访问策略的执行,管理简单快捷。

(2) 思科 Cisco。

思科可能是历史上最有名的网络公司。其防火墙产品特性如下:

① 可在单一设备中集成丰富的安全服务。使用专用的安全操作系统,消除了各种安全风险,提高可靠性。

② 安全功能强大,可综合利用各种先进技术。

③ 支持IKE和IPSec VPN标准。

④ 融合了入侵检测的功能。还可与思科网络入侵解决方案相集成,构成统一的网络防护体系。

⑤ 提供动态或者静态的网络地址解析(NAT)和端口地址解析(PAT)功能。

⑥ 用户可灵活地实现联网功能而且与PPPoE(PPP Over Ethernet)网络兼容。

⑦ 管理方便、快捷,手段灵活,提供了较强的可管理性和可审计性。

(3) 天融信。

天融信公司于1996年推出了中国第一套自主版权的防火墙产品,填补了国内防火墙产品的空白。随后几年又推出了VPN、IDS、过滤网关、安全审计、安全管理等一系列安全相关产品。

天融信公司的银河防火墙(NGFW4000-UF TG-5736)是国内首款具备万兆网络接入能力的防火墙产品。网络卫士猎豹系列防火墙则采用了具有国产知识产权的新一代可编程安全芯片。

(4) WatchGuard。

美国WatchGuard公司是全球排名前五位的专业生产防火墙的公司之一。WatchGuard公司以生产即插即用Internet安全设备“Firebox”系列和相应的服务器安全软件而闻名于世。

其产品包括从高端到低端的Firebox X Peak、Firebox X Core和Firebox X Edge三大系列,均具有防火墙、VPN、网关防毒、入侵防御、网站分类过滤(WebBlocker)、垃圾邮件拦截(SpamBlocker)、反间谍软件等多项网络安全与内容安全防御功能。三个系列的主要区别是应用环境不同:Firebox X Peak系列适用于高级网络环境,Firebox X Core系列适用于公司和分支机构,Firebox X Edge系列适用于中小型企业、远程办公室和远程工作人员。

WatchGuard的产品具有高安全性、易用性、较高的性价比等特点。

(5) 东软。

东软的 NetEye 防火墙(FW)产品采用独创的基于状态包过滤的“流过滤”体系结构，保证了从数据链路层到应用层的完全高性能过滤，并可以进行应用级插件的及时升级和安全威胁的有效防护，实现网络安全的动态保障。

NetEye 防火墙采用 NP 架构，运行于 NetEye 安全操作系统之上，具有高吞吐量、低延迟、零丢包率和强大的缓冲能力。同时 NetEye 防火墙集成 VPN 功能，简单及人性化的虚拟通道设置，有效提高了 VPN 的部署灵活性和可扩展性，降低了部署维护的成本。

除此之外还有 CheckPoint、安氏、飞塔 Fortinet 等知名的防火墙厂商。

2. 常用的软件防火墙产品

个人软件防火墙软件是一种能够保护个人计算机系统安全的软件，它可以直接在用户的计算机上运行，保护一台计算机免受攻击。常用的个人软件防火墙产品有天网个人防火墙、江民黑客防火墙、瑞星个人防火墙和 Windows 自带的防火墙等。

天网防火墙(SkyNet-FireWall)是一款由天网安全实验室制作的给个人计算机使用的网络安全程序。它根据系统管理者设定的安全规则(security rules)把守网络，提供强大的访问控制、应用选通、信息过滤等功能。

江民黑客防火墙，界面风格简单明了，常用的功能都可以方便地进行设置，彻底阻挡黑客攻击、木马程序等网络危险，保护上网账号、QQ 密码、游戏分值等重要信息不被盗窃。

瑞星个人防火墙，为个人计算机提供全面的保护，有效地监控任何网络连接。通过过滤不安全的服务，防火墙可以极大地提高单机在网络环境中的安全，使系统能抵御非法的入侵，防止个人计算机和数据遭到破坏。

7.5 入侵检测技术

根据入侵的定义，一般将入侵行为定义为系统内部发生的任何违反安全策略的事件，具体包括对系统的非授权访问、授权用户超越其权限的访问、合法用户的非法访问、恶意程序的攻击及对系统配置信息和安全漏洞的探测等。

入侵检测是指通过对行为、安全日志、审计数据或网络上可以获得的信息进行操作，检测到对系统的入侵行为或入侵的企图。它包括对系统的非法访问和越权访问的检测；包括监视系统运行状态，以发现各种攻击企图、攻击行为或者攻击结果；还包括针对计算机系统或网络的恶意试探的检测。而上述各种入侵行为的判定，即检测的操作，是通过在计算机系统或网路的各个关键点上收集数据并进行分析来实现的。1997 年，美国国家安全通信委员会(NSTAC)下属的入侵检测小组(IDSG)给出了一个入侵检测的经典定义，即入侵检测是对企图入侵、正在进行的入侵或者已经发生的入侵进行识别的过程。

入侵检测技术是指进行数据采集与分析进而检测出入侵行为的相关技术，入侵检测系统是使用入侵检测技术执行入侵检测任务的软、硬件或者软件与硬件相结合的系统。假如防火墙是一幢大楼的门卫，那么入侵检测系统就是这幢大楼里的实时监视系统。一

旦小偷爬窗进入大楼，或内部人员有越界行为，实时监视系统就能发现情况并发出警告。

本节主要介绍入侵检测技术、入侵检测过程与入侵检测系统等方面的内容。

7.5.1 入侵检测的分类

入侵检测技术是由于检测入侵行为的迫切性而产生的，是保证计算机系统安全设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机系统与网络中违反安全策略行为的技术。

1. 入侵检测技术的分类

入侵检测技术可以分为基于标识（signature-based）与基于异常情况（anomaly-based）两种类型。

（1）对于基于标识的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。此方法非常类似杀毒软件。

（2）基于异常的检测技术则是先定义一组系统"正常"情况的数值，如 CPU 利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统，并用统计的办法得出），然后将系统运行时的数值与所定义的"正常"情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的"正常"情况。

使用这两种不同的检测技术，可能会得出不同的结论。基于标志的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法，但它可以（至少在理论上可以）判别更广泛，甚至未发觉的攻击。因此，两种技术可以结合使用。

2. 入侵检测新技术

入侵检测技术还包括适合大规模数据分析和内容提取的数据挖掘技术、具有自修复和自学习能力的计算机免疫学技术、具备知识更新和学习能力的神经网络技术以及具备优化能力的遗传算法等。这些新技术的应用可以提高入侵检测系统对于多种复杂的入侵行为的探测、识别和响应能力，能够大大增强用户系统的安全性。

7.5.2 入侵检测的过程

检测入侵行为的过程主要分为三步：信息收集、信号分析和结果处理。

1. 信息收集

信息收集的内容主要包括系统、网络、数据及用户活动的状态和行为。信息收集需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息。因为从一个源来的信息有可能看不出疑点，但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。当然，入侵检测很大程度上依赖于收集信息的可靠性和正确性，因此，要使用有

安全保证的软件来报告这些信息。因为黑客经常替换软件以搞混和移走这些信息，例如替换被程序调用的子程序、库和其他工具。黑客对系统的修改可能使系统功能失常并看起来跟正常的一样。例如，UNIX 系统的 PS 指令可以被替换为一个不显示侵入过程的指令，或者是编辑器被替换成一个读取不同于指定文件的文件(黑客隐藏了初始文件并用另一个版本代替)。

为入侵检测收集的信息一般来自以下四个方面：

(1) 系统和网络日志文件；

(2) 目录和文件中的不期望的改变；

(3) 程序执行中的不期望行为；

(4) 物理形式的入侵信息。

2. 信号分析

信号分析是指对收集到的有关系统、网络、数据及用户活动状态和行为等的信息通过技术手段进行分析的过程。信号分析的技术手段有三种：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，完整性分析则用于事后分析。

(1) 模式匹配。

模式匹配就是将接收到的信息与已知的网络入侵特征库中的数据进行比较，检查接收到的数据中是否包含特征库中的攻击特征，从而判断是否受到攻击。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令)，也可以很复杂（如利用正规的数学表达式来表示安全状态的变化)。一般来讲，一种进攻模式可以用一个过程（如执行一条指令)或一个输出（如获得权限)来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断地升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

(2) 统计分析。

统计分析方法首先给系统对象（如用户、文件、目录和设备等)创建一个统计描述，统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚八点至早六点不登录的账户却在凌晨两点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法，目前正处于研究热点和迅速发展之中。

(3) 完整性分析。

完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的、被特洛伊化的应用程序方面特别有效。完整性分析利用强有力的加密机制，称为消息摘要函数（例如 MDS)，能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整

性检测方法也是网络安全产品的必要手段之一。例如，可以在每一天的某个特定时间内开启完整性分析模块，对网络系统进行全面的扫描检查。

3. 结果处理

结果处理是指当检测到入侵时，就产生预先定义的响应，并采取相应的措施。可以是重新配置路由器或防火墙、终止进程、切断连接、改变文件属性，也可以只是简单的警告。

7.5.3 入侵检测系统

用于入侵检测的软硬件组合称为入侵检测系统（intrusion detection system，IDS），它被认为是防火墙之后的第二道安全闸门，它能监视分析用户及系统活动，查找用户的非法操作，评估重要系统和数据文件的完整性，检测系统配置的正确性，提示管理员修补系统漏洞；能实时地对检测到的入侵行为进行反应，在入侵攻击对系统发生危害前利用报警与防护系统驱逐入侵攻击，在入侵攻击过程中减少入侵攻击所造成的损失，在被入侵攻击后收集入侵攻击的相关信息，作为防范系统的知识，添加到入侵策略集中，增强系统的防范能力，避免系统再次受到同类型的入侵攻击。

1. 入侵检测系统的目标与功能

（1）入侵检测系统的目标。

入侵检测系统是对计算机和网络资源的恶意使用行为进行识别和相应处理的系统，它的目标是依照一定的安全策略，对网络、系统的运行状况进行监视，及时发现各种攻击企图、行为或结果，以保证网络系统资源的机密性、完整性和可用性。

（2）入侵检测系统的功能。

① 监视、分析用户及系统的活动；

② 系统构造和弱点的审计；

③ 识别反映已知进攻的活动模式并向相关人士报警；

④ 异常行为模式的统计分析；

⑤ 评估重要系统和数据文件的完整性；

⑥ 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

2. 入侵检测系统的组成

IETF（internet engineering task force，Internet 工程任务组）将一个入侵检测系统分为四个组件：事件产生器（event generators）；事件分析器（event analyzers）；响应单元（response units ）；事件数据库（event databases）。

（1）事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

（2）事件分析器分析得到的数据，并产生分析结果。

（3）响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。

（4）事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

四个组件的关系如图 7-7 所示。

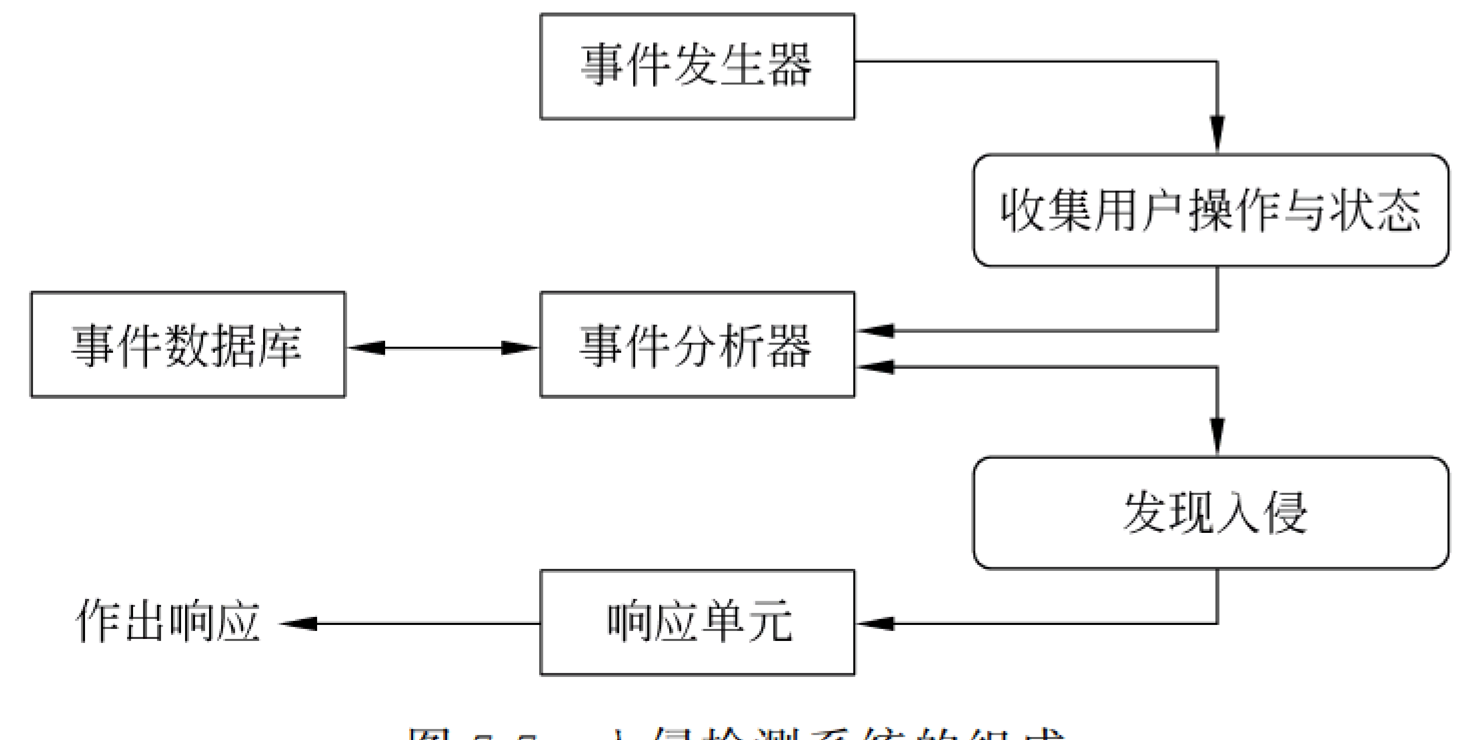


图 7-7　入侵检测系统的组成

3．入侵检测系统的作用

（1）识别黑客常用攻击手段。

入侵检测系统通过分析各种攻击的特征，可以全面快速地识别探测攻击、拒绝服务攻击、缓冲区溢出攻击等各种常用攻击手段，并采取相应的措施。

（2）监控网络异常通信。

入侵检测系统会对网络中不正常的通信连接做出反应，保证网络通信的合法性；任何不符合网络安全策略的网络数据都会被入侵检测系统侦测到并警告。

（3）鉴别对系统漏洞及后门的利用。

入侵检测系统一般带有系统漏洞及后门的详细信息，通过对网络数据包连接的方式、连接端口以及连接中特定的内容等特征分析，可以有效地发现网络通信中针对系统漏洞进行的非法行为。

（4）完善网络安全管理。

入侵检测系统通过对攻击或入侵的检测及反应，可以有效地发现和防止大部分的网络犯罪行为，给网络安全管理提供一个集中、方便、有效的工具。使用入侵检测系统的监测、统计分析、报表功能，可以进一步完善网络管理。

对一个成功的入侵检测系统来讲，它不但可以使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制定提供指南。更为重要的一点是，它应该管理、配置简单，从而使非专业人员能够非常容易地获得网络安全。入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现攻击后，会及时做出响应，包括切断网络连接、记录事件和报警等。

4．入侵检测系统分类

（1）以采用的技术分类。

入侵检测系统根据其采用的技术可以分为异常检测和特征检测。

① 异常检测：异常检测的假设是入侵者活动异常于正常主体的活动，建立正常活动的“活动简档”，当前主体的活动违反其统计规律时，认为可能是“入侵”行为。通过检测系统的行为或使用情况的变化来完成。

② 特征检测：特征检测假设入侵者活动可以用一种模式来表示，然后将观察对象与之进行比较，判别是否符合这些模式。

(2) 以监测的对象分类。

入侵检测系统根据其监测的对象主机、网络与混合，分为基于主机、基于网络和混合型三类。

① 基于主机：系统分析的数据是计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录。主机型入侵检测系统保护的目标是所在的主机系统，通过监视与分析主机的数据检测入侵，其任务由代理(agent)来实现，代理是运行在目标主机上的可执行程序，它们与命令控制台(console)通信。能否及时采集到审计数据是这些系统的弱点之一，入侵者会将主机审计子系统作为攻击目标以避开入侵检测系统。

② 基于网络：系统分析的数据是网络上的数据包。网络型入侵检测系统担负着保护整个网段的任务，基于网络的入侵检测系统由遍及网络的传感器(sensor)组成，传感器是一台将以太网卡置于混杂模式的计算机，用于嗅探网络上的数据包，通过侦听采集的数据，分析可疑现象。这类系统不需要主机提供严格的审计，对主机资源消耗少，并可以提供对网络通用的保护而无须顾及异构主机的不同架构。

③ 混合型：基于网络和基于主机的入侵检测系统都有不足之处，会造成防御体系的不全面，综合了基于网络和基于主机的混合型入侵检测系统既可以发现网络中的攻击信息，也可以从系统日志中发现异常情况。

5. 入侵检测系统的部署

一般入侵检测产品都由传感器和控制台两个部分组成。传感器负责采集、分析数据并生成安全事件，控制台主要起到中央管理的作用。基于网络的入侵检测系统需要有传感器才能工作。入侵检测系统的部署主要是传感器位置的部署。如果传感器放的位置不正确，入侵检测系统也无法工作在最佳状态，一般可以采取以下 4 个选择：

(1) 放在边界防火墙之内，传感器可以发现所有来自 Internet 的攻击，然而如果攻击类型是 TCP 攻击，而防火墙或过滤路由器能封锁这种攻击，那么入侵检测系统可能检测不到这种攻击的发生。

(2) 放在边界防火墙之外，可以检测所有对保护网络的攻击事件，包括数目和类型。但是这样部署会使传感器彻底地暴露在黑客之下。

(3) 放在主要的网络中枢中，传感器可以监控大量的网络数据，可提高检测黑客攻击的可能性，可通过授权用户的权利来发现未授权用户的行为。

(4) 放在一些安全级别需求高的子网中，对非常重要的系统和资源的入侵检测，例如一个公司的财务部门，这个网段安全级别需求非常高，因此可以对财务部门单独放置一个检测器系统。

7.5.4　主流入侵检测产品

近年来，国内外厂家和研究机构推出了不少入侵检测产品，如 Internet Security System 公司的 RealSecure，Cisco 思科公司的 NetRanger，Network Associates 公司的 CyberCop，这些产品有的已得到广泛应用，有的是免费产品，有的是非商用产品，下面简单介绍一下这些产品。

1．Cisco 思科公司的 NetRanger

1996 年 3 月，思科公司推出了 NetRanger。产品分为两部分：监测网络包和发警告的传感器，以及接收并分析警告和启动对策的控制器。产品有以下特点：

（1）可以综合多站点的信息。

NetRanger 的控制器程序可以综合多站点的信息，监视散布在整个企业网上的攻击。

（2）有路径备份功能。

如果监测的路径上有一条断掉了，信息可以从备份路径上传过来。NetRanger 甚至能做到从一个点上监测全网或把监测权转给第三方。

（3）监测问题时不仅观察单个包的内容，还要看上下文。

NetRanger 可以从多个包中发现线索。这是很重要的一点，因为入侵者可能以字符模式存取一个端口，然后在每个包中只放一个字符。如果一个监测器只观察单个包，它就永远不会发现完整的信息。

2．Network Associates 公司的 CyberCop

Network Associates 公司是 1977 年由以做 Sniffer 类探测器闻名的 Network General 公司与以做反病毒产品为专业的 McAfee Associates 公司合并而成的。NetWork Associates 公司从 Cisco 公司那里取得授权，将 NetRanger 的引擎和攻击模式数据库用在 CyberCop 中。CyberCop 可以认为是 NetRanger 的局域网管理员版。

CyberCop 被设计成一个网络应用程序，易于安装。它预设了 6 种通常的配置模式：Windows NT 与 UNIX 的混合子网、UNIX 子网、NT 子网、远程访问、前沿网（如 Internet 的接入系统）和骨干网。

CyberCop 的前端为浏览器方式，用户易于查看和理解。在帮助文档里还结合了专家知识。CyberCop 还能生成可以被 Sniffer 识别的踪迹文件。但与 NetRanger 相比，CyberCop 缺乏一些企业应用的特征，如路径备份功能等。

3．ISS 公司的 RealSecure

ISS（internet security system，国际互联网安全系统）公司的 RealSecure 是计算机网络上自动实时的入侵检测和响应系统。它无妨碍地监控网络传输并自动检测和响应可疑的行为，在系统受到危害之前截取和响应安全漏洞和内部误用，从而最大程度地为企业网络提供安全。

RealSecure 的优势还在于其简洁性和低价格。与 NetRanger 和 CyberCop 类似，

RealSecure 在结构上也是两部分。引擎部分负责监测信息包并生成告警，控制台接收报警并作为配置及产生数据库报告的中心点。两部分都可以在 NT、Solaris、SunOS 和 Linux 上运行，并可以在混合的操作系统或匹配的操作系统环境下使用。RealSecure 的一个引擎可以向多个控制台报告，一个控制台也可以管理多个引擎，并且这两部分都能在商用计算机上运行。

4. Intrusion Detection 公司的 Kane Security Monitor

基于主机的 Kane Security Monitor(KSM)是 1997 年 9 月推出的。它在结构上由三部分组成，即审计器、控制台和代理。它在每个要保护的主机上运行一个代理程序。代理用来浏览主机的日志并将统计结果送往审计器。系统安全员用控制台的 GUI 界面来接收告警、查看历史记录以及系统的实时行为。

7.6 蜜罐与蜜网技术

与其他安全防护技术数据加密技术、认证技术、防火墙技术、入侵检测技术、病毒防护技术不同，这些技术多数都是在攻击者对网络进行攻击时进行的被动防护，蜜罐(honeypot)与蜜网技术采取的是主动防护。蜜罐与蜜网技术是主动引诱攻击者攻击与入侵，借此收集证据，同时对攻击者的各种攻击行为进行分析并找到有效的对付办法。

本节主要介绍蜜罐技术的基本概念、蜜罐的类型、蜜罐的配置模式，并对蜜网进行简单说明。

7.6.1 蜜罐的基本概念

1. 蜜罐的产生

入侵检测系统(IDS)能够对网络和系统的活动情况进行监视，及时发现并报告异常现象。但是，入侵检测系统在使用中存在着难以检测新类型黑客攻击方法，可能漏报和误报的问题。

蜜罐技术使这些问题得到进一步的解决，通过观察和记录黑客在蜜罐上的活动，人们可以了解黑客的动向、黑客使用的攻击方法等有用信息。如果将蜜罐采集的信息与 IDS 采集的信息联系起来，则有可能减少 IDS 的漏报和误报，并能用于进一步改进 IDS 的设计，增强 IDS 的检测能力。

蜜罐的思想最早是由 Clifford Stoll 于 1988 年 5 月提出的，该作者在跟踪黑客的过程中，利用了一些包含虚假信息的文件作为黑客"诱饵"来检测入侵，这就是蜜罐的基本构想，但它并没有提供一个专门让黑客攻击的系统。

蜜罐正式出现是 Bill Cheswick 提到采用服务仿真和漏洞仿真技术来吸引黑客。服务仿真技术是蜜罐作为应用层程序打开一些常用服务端口监听，仿效实际服务器软件的行为响应黑客请求。例如，提示访问者输入用户名和口令，从而吸引黑客进行登录尝试。所谓漏洞仿真是指返回黑客的响应信息会使黑客认为该服务器上存在某种漏洞，从而引

诱黑客继续攻击。

2. 蜜罐的定义

美国著名的蜜罐技术专家 L. Spizner 对蜜罐做了这样的定义：蜜罐是一种资源，它的价值是被攻击或攻陷。

蜜罐是一种专门设计成被扫描、攻击和入侵的资源，它的目的就是建立一个诱骗环境吸引攻击者和入侵者，观察并且以日志的形式记录其在里面的活动，并且使攻击者在蜜罐中耗费精力和技术，从而保护了真正有价值的正常的系统和资源。

以上定义意味着蜜罐是用来被探测、被攻击甚至最后被攻陷的，蜜罐不会修补任何东西，这样就为使用者提供了额外的、有价值的信息。蜜罐不会直接提高计算机网络安全，但是它却是其他安全策略所不可替代的一种主动防御技术。

3. 蜜罐的组成

蜜罐由一台不作任何安全防范措施连接网络的计算机和一套网络监控系统组成，它与一般计算机不同，其内部运行着多种多样的数据记录程序和特殊用途的“自我暴露程序”，就像要诱惑贪嘴的黑熊上钩，蜂蜜是不可少的。监控系统用来记录进出计算机的所有流量。

4. 蜜罐的功能

设计蜜罐的目的就是让黑客入侵，借此收集证据，同时隐藏真实的服务器地址，一台合格的蜜罐要拥有如下功能。

(1) 吸引攻击者入侵。蜜罐是故意让人攻击的目标，引诱黑客前来攻击。通常在蜜罐系统上留下一些安全后门以吸引攻击者上钩，或者放置一些网络攻击者希望得到的敏感信息，当然这些信息都是虚假的信息。

(2) 对系统中所有操作和行为进行监视和记录。通过精心的伪装，使得攻击者在进入到目标系统后仍不知道自己所有的行为已经处于系统的监视下。

(3) 收集情报。根据攻击者的入侵记录，可以发现黑客是如何得逞的，以此随时了解针对服务器发动的最新攻击和漏洞。通过蜜罐还可以窃听黑客之间的联系，收集黑客所用的攻击工具，掌握他们的社交网络。通过分析攻击者的聊天内容记录，可以发现攻击者采用的攻击目的、攻击手段和攻击水平等信息，了解攻击者的活动范围以及下一个攻击目标。

(4) 收集证据。在必要的时候根据蜜罐收集的证据管理员可以起诉入侵者。

5. 蜜罐的优势

(1) 能够发现新的攻击工具与方法。

(2) 数据量小。

与 IDS 相比较，蜜罐仅仅收集那些对它进行访问的数据。在同样的条件下，IDS 可能会记录成千上万的报警信息，而蜜罐却只有几百条。这就使得蜜罐收集信息更容易，分析

起来也更为方便。

(3) 减少误报率。

与 IDS 相比较，蜜罐能显著减少误报率。任何对蜜罐的访问都是未授权的、非法的，这样蜜罐检测攻击就非常有效，从而大大减少了错误的报警信息，甚至可以避免。这样网络安全人员就可以集中精力采取其他的安全措施。

(4) 捕获漏报。

蜜罐可以很容易地鉴别捕获针对它的新的攻击行为。由于针对蜜罐的任何操作都不是正常的，这样就使得任何新的以前没有见过的攻击很容易暴露。

(5) 资源最小化。

蜜罐所需要的资源很少，即使工作在一个大型网络环境中也是如此。一个简单的 Pentium 主机就可以模拟具有多个 IP 地址的 C 类网络。

(6) 技术简单。

相对入侵检测及其他技术，蜜罐技术简单，容易掌握。

6. 蜜罐技术的法律问题

需要注意的是监控蜜罐也要承担相应的法律后果，譬如说，有可能违反《反窃听法》。虽然目前没有判例，但熟悉这方面法律的人士大多数认为，双方同意的标语是该问题的解决出路。也就是说，给每个蜜罐打上这样的标语："使用该系统的任何人同意自己的行为受到监控，并透露给其他人，包括执法人员。"

7.6.2 蜜罐的分类

研究人员和安全专家使用的蜜罐工具各种各样，根据不同的标准可以对蜜罐技术进行不同的分类。

1. 以设计的最终目的分类

根据设计的最终目的不同可以将蜜罐分为产品型蜜罐和研究型蜜罐两类。

(1) 产品型蜜罐一般运用于商业组织的网络中。它的目的是减轻受保护组织将受到的攻击的威胁，蜜罐加强了受保护组织的安全措施。它们所做的工作就是检测并且对付恶意的攻击者。

(2) 研究型蜜罐专门以研究和获取攻击信息为目的而设计。这类蜜罐并没有增强特定组织的安全性，恰恰相反，蜜罐要做的是让研究组织面对各类网络威胁，并寻找能够对付这些威胁更好的方式，它们所要进行的工作就是收集恶意攻击者的信息。它一般运用于军队和安全研究组织。

2. 以蜜罐与攻击者之间进行的交互方式分类

根据蜜罐与攻击者之间进行的交互方式，可以分为 3 类：低交互蜜罐，中交互蜜罐和高交互蜜罐，同时这也体现了蜜罐发展的 3 个过程。

(1) 低交互蜜罐最大的特点是模拟。蜜罐为攻击者展示的所有攻击弱点和攻击对象都不是真正的产品系统,而是对各种系统及其提供的服务的模拟。由于它的服务都是模拟的行为,所以蜜罐可以获得的信息非常有限,只能对攻击者进行简单的应答,它是最安全的蜜罐类型。

(2) 中交互是对真正的操作系统的各种行为的模拟,它提供了更多的交互信息,同时也可以从攻击者的行为中获得更多的信息。在这个模拟行为的系统中,蜜罐可以看起来和一个真正的操作系统没有区别。

(3) 高交互蜜罐具有一个真实的操作系统,它的优点体现在对攻击者提供真实的系统,当攻击者获得 ROOT 权限后,受系统与数据真实性的迷惑,他的更多活动和行为将被记录下来。缺点是被入侵的可能性很高,如果整个蜜罐被入侵,那么它就会成为攻击者下一步攻击的跳板。

7.6.3 蜜罐的配置模式

1. 诱骗服务(deception service)

诱骗服务是指在特定的 IP 服务端口侦听并像应用服务程序那样对各种网络请求进行应答的应用程序。DTK 就是这样的一个服务性产品。DTK 吸引攻击者的诡计就是可执行性,但是它与攻击者进行交互的方式是模仿那些具有可攻击弱点的系统进行的,所以可以产生的应答非常有限。在这个过程中对所有的行为进行记录,同时提供较为合理的应答,并给闯入系统的攻击者带来系统并不安全的错觉。例如,将诱骗服务配置为 FTP 服务的模式。当攻击者连接到 TCP/21 端口的时候,就会收到一个由蜜罐发出的 FTP 的标识。如果攻击者认为诱骗服务就是他要攻击的 FTP,他就会采用攻击 FTP 服务的方式进入系统。这样,系统管理员便可以记录攻击的细节。

2. 弱化系统(weakened system)

只要在外部因特网上有一台计算机运行没有打上补丁的微软 Windows 或者 Red Hat Linux 即行。这样的特点使攻击者更加容易进入系统,系统可以收集有效的攻击数据。因为黑客可能会设陷阱,以获取计算机的日志和审查功能,需要运行其他额外记录系统,实现对日志记录的异地存储和备份。它的缺点是“高维护低收益”。因为,获取已知的攻击行为是毫无意义的。

3. 强化系统(hardened system)

强化系统同弱化系统一样,提供一个真实的环境。不过此时的系统已经武装成看似足够安全的。当攻击者闯入时,蜜罐就开始收集信息,它能在最短的时间内收集最多有效数据。用这种蜜罐需要系统管理员具有更高的专业技术。如果攻击者具有更高的技术,那么,他很可能取代管理员对系统的控制,从而对其他系统进行攻击。

4. 用户模式服务器(user mode server)

用户模式服务器实际上是一个用户进程,它运行在主机上,并且模拟成一个真实的服

务器。在真实主机中，每个应用程序都当作一个具有独立 IP 地址的操作系统和服务的特定实例。而用户模式服务器这样一个进程就嵌套在主机操作系统的应用程序空间中，当 Internet 用户向用户模式服务器的 IP 地址发送请求，主机将接受请求并且转发到用户模式服务器上。

这种模式的成功与否取决于攻击者的进入程度和受骗程度。它的优点体现在系统管理员对用户主机有绝对的控制权。即使蜜罐被攻陷，由于用户模式服务器是一个用户进程，那么只要关闭该进程就可以了。另外就是可以将防火墙、IDS 集中于同一台服务器上。当然，其局限性是不适用于所有的操作系统。

7.6.4 蜜网简介

1. 蜜网的产生

蜜罐是一种安全资源，其价值在于被扫描、攻击和攻陷。传统蜜罐有着不少的优点，例如收集数据的保真度，蜜罐不依赖于任何复杂的检测技术等，因此减少了漏报率和误报率。使用蜜罐技术能够收集到新的攻击工具和攻击方法，而不像目前的大部分入侵检测系统只能根据特征匹配的方法检测到已知的攻击。

但是随着应用的广泛，传统蜜罐的缺点也开始暴露了出来，综合起来主要有 3 个方面：

(1) 蜜罐技术只能对针对蜜罐的攻击行为进行监视和分析，其视图不像入侵检测系统能够通过旁路侦听等技术对整个网络进行监控。

(2) 蜜罐技术不能直接防护有漏洞的信息系统并有可能被攻击者利用带来一定的安全风险。

(3) 攻击者在加密通道上进行的活动增多，数据捕获后需要花费时间破译，这给分析攻击行为增加了困难。

针对以上问题出现了蜜网技术。蜜网技术实质上是一类研究型的高交互蜜罐技术，与传统蜜罐技术的差异在于，蜜网构成了一个黑客诱捕网络体系架构，在这个架构中，可以包含一个或多个蜜罐，同时保证了网络的高度可控性，以及提供多种工具以方便对攻击信息的采集和分析。一般蜜网的网络拓扑结构如图 7-8 所示。

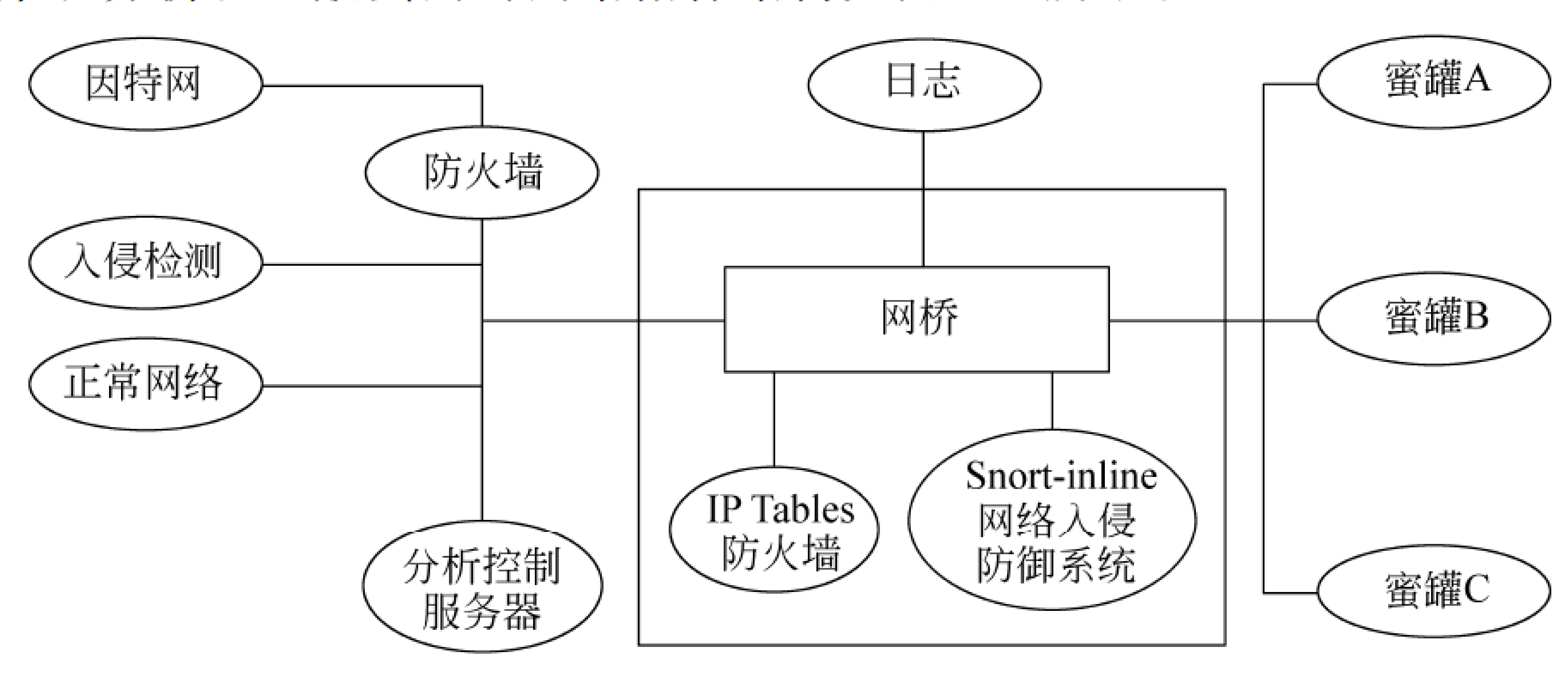


图 7-8 蜜网的网络拓扑结构图

2. 蜜网的三大核心需求

蜜网有三大核心需求：数据控制、数据捕获和数据分析。

（1）数据控制就是限制攻击者活动的机制，通过数据控制能够确保黑客不能利用蜜网危害第三方网络的安全，以减轻蜜网架设的风险，降低安全风险。

（2）数据捕获就是监控和记录所有攻击者在蜜网内部的活动，包括记录加密会话中的击键，恢复使用 SCP 命令拷贝的文件，捕获远程系统被记录的口令，恢复使用保护的二进制程序的口令等。这些捕获的数据将会被用于分析，从中发现黑客界成员们使用的工具、策略以及他们的动机。

（3）数据分析是指安全研究人员从捕获的数据中分析出黑客的攻击行动、使用工具及其意图。

3. 蜜网的应用

（1）抗蠕虫病毒。

蠕虫的一般传播过程为扫描、感染、复制三个步骤。经过大量扫描，当探测到存在漏洞的主机时，蠕虫主体就会迁移到目标主机。然后在被感染的主机上生成多个副本，实现对计算机的监控和破坏。利用蜜网技术，可以在蠕虫感染的阶段检测非法入侵行为，对于已知蠕虫病毒，可以通过设置防火墙和入侵检测系统规则，直接重定向到蜜网的蜜罐中，拖延蠕虫的攻击时间；对于全新的蠕虫病毒，可以采取办法延缓其扫描速度，在网络层用特定的、伪造的数据包来延迟应答，同时利用软件工具对日志进行分析，以便确定相应的对抗措施。

（2）捕获网络钓鱼。

网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息的一种攻击方式。目前的反网络钓鱼工作组等机构寄希望于发觉网络钓鱼攻击的用户向他们报告，通过报告再进行分析。这种途径只能在网络钓鱼攻击发生后从受害者的角度去观察，并不能清晰地了解网络钓鱼攻击的全过程。蜜网技术则提供了捕获整个过程中攻击者发起攻击行为的能力，在蜜网中的蜜罐都是初始安装的没有打漏洞补丁的系统，一旦部署的蜜网被网络钓鱼者以进行网络钓鱼攻击，安全分析人员就能及时在蜜网捕获的丰富日志数据的基础上，对网络钓鱼攻击的整个生命周期建立起一个完整的理解，并深入剖析各个步骤钓鱼者所使用的技术手段和工具。

（3）捕获僵尸网络。

僵尸网络是近年来兴起的危害 Internet 的重大威胁之一，它的危害体现在发动分布式拒绝服务攻击、发送垃圾邮件以及窃取僵尸主机内的敏感信息等。因此，可以考虑利用在网络中部署恶意软件收集器，对收集到的恶意软件样本采用蜜网技术对其进行分析，确认是否僵尸程序，并对僵尸程序所要连接的僵尸网络控制信道的信息进行提取，最后通过客户端蜜罐技术，伪装成被控制的僵尸工具，进入僵尸网络进行观察和跟踪。

4. 蜜网的发展趋势

(1) 提高蜜网的可移植性。

目前的操作系统各种各样,大部分蜜网只能够在特定的操作系统下工作。因此,能够跨平台工作的蜜网成为安全工作者关注的焦点。如果蜜网可以在任何操作系统下生效,蜜网的适用范围变得更宽,使用者的范围就会不断增加。

(2) 提高蜜网的交互性。

在尽量降低风险的情况下,提高蜜网与入侵者之间的交互程度。蜜网如果仅仅支持简单的交互行为,就可能被入侵者很快发现并迅速全身而退。所以蜜网技术不断进步的过程中,必须尽量提高与入侵者之间的交互程度,以便更好地了解入侵者行为并得出结论。

(3) 提高蜜网的信息控制和记录功能。

当前的蜜网技术在记录攻击者攻陷一台计算机之后的情况方面还做得很不够。因为大规模分布式的攻击成为一种攻击"时尚",了解攻击者在攻陷一台计算机之后的所作所为,成为安全工作必不可少的一部分,也是蜜罐的重要工作。

(4) 降低蜜网的风险。

如何降低蜜网引入的风险,一直都是蜜网使用者们关注的问题之一,想要获得更多的有价值的信息和数据,又要系统保持足够的安全,这的确很难。交互的程度越高,模拟得越像,自己陷入危险的概率就越大。

7.7 应用实例

针对上述主要的网络攻击防御技术,本节将介绍三种技术的具体应用。其中包括配置 Windows 7 中的防火墙,安装和使用 Snort 入侵检测系统,以及建立简单的蜜罐。

7.7.1 配置 Windows 7 中的防火墙

从 Windows XP 开始,Windows 系统就自带防火墙,防止黑客或恶意软件通过网络入侵用户的计算机。经过 Windows Vista 的发展,Windows 7 中的防火墙日臻完善。首先,通过控制面板中的选项就可以直观地完成防火墙的所有设置,界面简洁清晰。再者,Windows 7 的防火墙中集成了高级安全 Windows 防火墙,能够更加专业、全面地进行防火墙策略配置。

下面介绍设置 Windows 7 中防火墙的方法与步骤。

1. 启动 Windows 7 中的防火墙

在 Windows 桌面,单击"开始"→"控制面板"菜单命令,打开"控制面板"对话框,双击"系统和安全"后选择"Windows 防火墙"选项,进入 Windows 防火墙的界面。Windows 7 中的防火墙界面如图 7-9 所示。

在这个界面中可以直观地看到当前计算机与不同网络的连接状态,以及相应的网络



图 7-9　Windows 7 防火墙界面

保护措施。图 7-9 界面上的“传入连接”表示网络中发来的数据包的目的地为本机(如即时通信软件接收文件),传出连接则表示数据包由本机发出(如应用程序连接某个网站)。对于普通用户而言,Windows 防火墙常规设置即可满足通常的安全需求。当然也可以自定义每种网络的防火墙设置,还可以选择允许通过防火墙的程序或功能。

2. 自定义不同类型网络的设置

通过对不同的网络位置使用不同的保护措施,可以更加灵活地保护计算机安全。例如,计算机在公用网络中面临的威胁往往多于家庭或工作网络,因此对于公用网络可以设置更加严格的传入连接规则,以获得更有保障的安全防护。具体操作步骤如下:

(1) 单击图 7-9 界面左侧的“更改通知设置”。这样即可针对每一种网络位置进行独立的设置,如图 7-10 所示。

(2) 选择“Windows 防火墙阻止新程序时通知我”选项。

3. 设置允许通过 Windows 防火墙的程序或功能

(1) 单击图 7-9 界面左侧的“允许程序或功能通过 Windows 防火墙”即可在程序和功能层面进行传入连接的规则设置,允许程序通过 Windows 防火墙通信设置窗口如图 7-11 所示。

(2) 选择允许某一程序或功能通过 Windows 防火墙通信,并且设置对一个或几个网络位置生效。如果需要添加另外的应用程序允许规则,可以单击右下角的【允许运行另一程序】按钮。

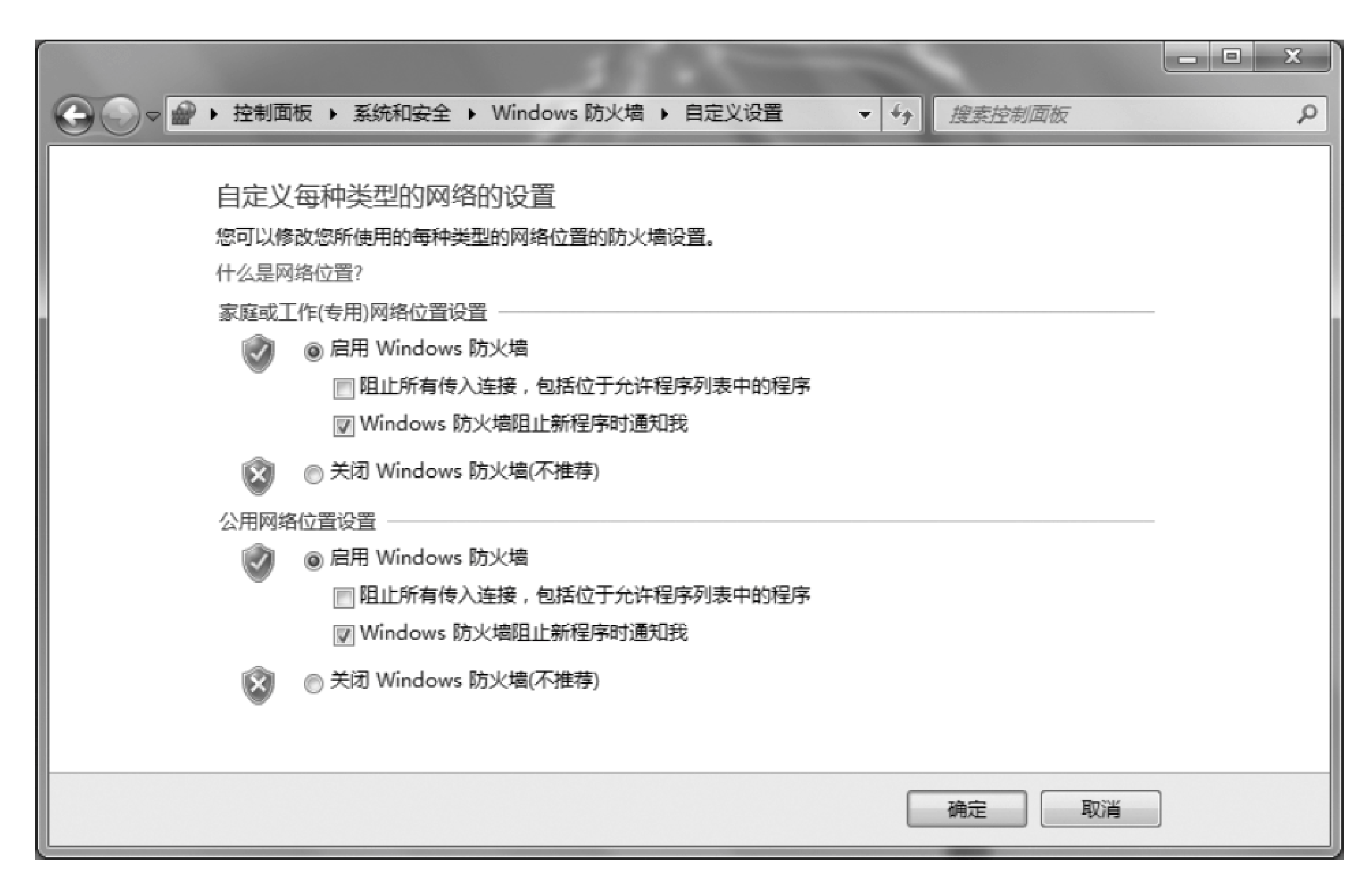


图 7-10　自定义不同类型网络的设置界面



图 7-11　“允许程序通过 Windows 防火墙通信”设置窗口

4. Windows 7 防火墙高级设置

在常规设置中已经可以选择某一程序或功能通过防火墙。如果需要对传入连接进行更加详细的规则定制，或者需要对传出连接也进行过滤，高级安全 Windows 防火墙可以做到。具体操作步骤如下：

单击图 7-9 界面左侧的“高级设置”即可进入高级安全 Windows 防火墙的设置窗口，如图 7-12 所示。



图 7-12　高级安全 Windows 防火墙窗口

5. 高级安全 Windows 防火墙属性设置

(1) 单击图 7-12 界面右侧“操作”下的“属性”标签即可进入属性设置窗口，如图 7-13 所示。



图 7-13　高级安全 Windows 防火墙属性设置窗口

防火墙属性设置可以对域、专用和公用配置文件进行设置，这三个配置文件分别应用

于域、专用和公用网络,以指定计算机连接到某个网络时的行为。

(2)“入站连接”选择“阻止”。

(3)“出站连接”选择“允许”,对于一些试图在用户不知情时连接外部某个网站的程序,可以通过添加例外的方式阻止该出站连接。

6. 高级安全 Windows 防火墙规则添加

高级安全 Windows 防火墙中可以使用入站规则和出站规则分别配置如何响应入站与出站连接,通过添加规则的方式就可以实现对一些例外程序的特殊处理。入站规则与出站规则的设置方法基本相同,这里以出站规则为例,设置步骤如下:

(1)单击图 7-12 窗口左侧的“出站规则”后,在弹出的对话框中单击“新建规则”即可进入“新建出站规则向导”窗口,如图 7-14 所示。



图 7-14 “新建出站规则向导”窗口

(2)选择需要创建的规则类型,若选择“自定义”则可以对所有的规则应用条件进行设置。

以上设置完成后,Windows 7 防火墙就能按用户的设置起到防御作用。例如用户运行了某个程序,该程序不在“通过 Windows 防火墙通信”的程序列表中,就会出现安全警报界面,如图 7-15 所示。

如果用户确定该程序没有危险,则单击【允许访问】。如果经常使用到该程序,可以把程序加到图 7-11“允许程序通过 Windows 防火墙通信”窗口的列表中。

7.7.2 安装和使用 Snort 入侵检测系统

除了前面介绍的入侵检测产品之外,还有一些优秀的入侵检测工具软件,如 Hostsentry、Portsentry、Tripwire,最为著名的就是 Snort,这些工具有的比较简单,有的

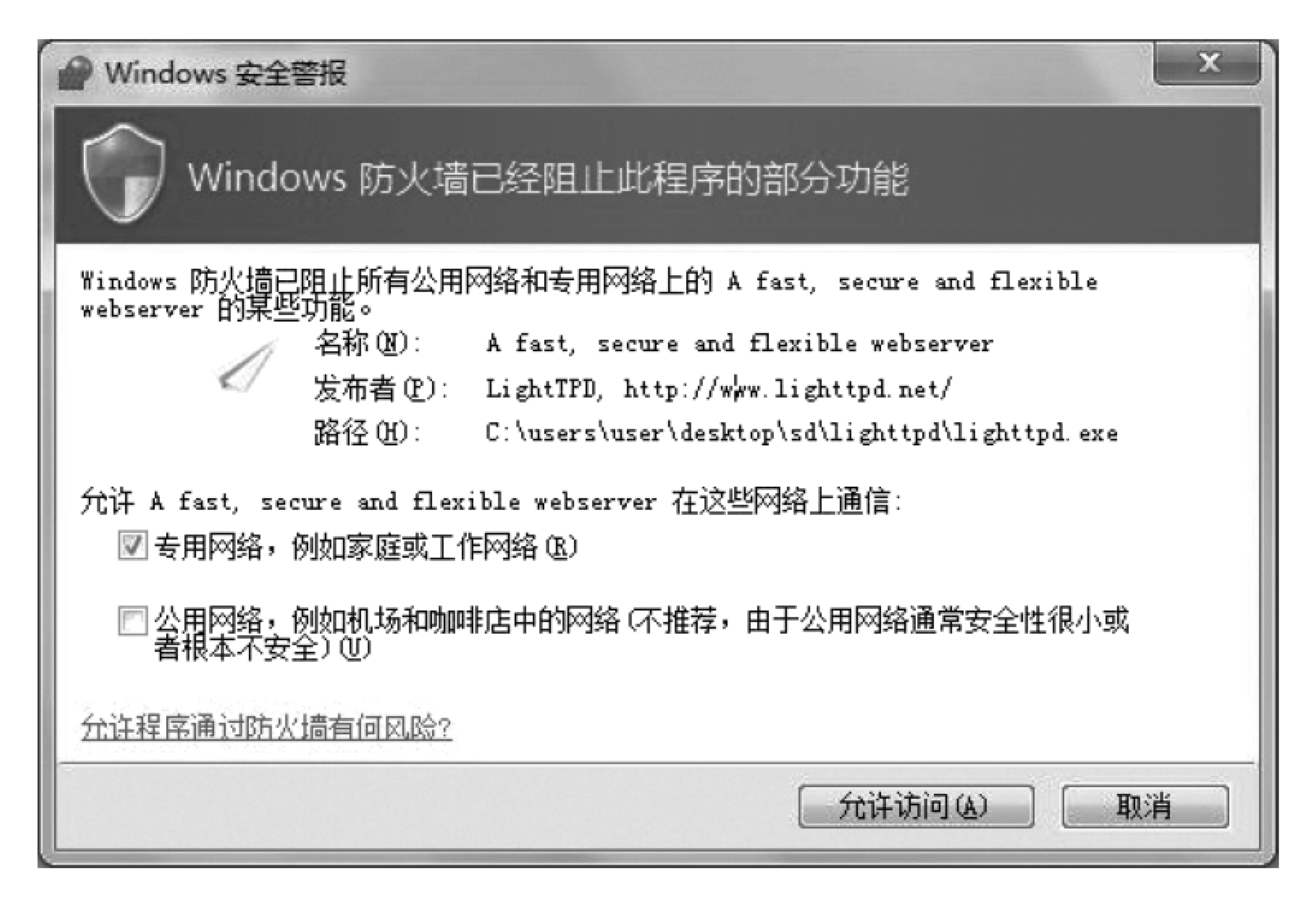


图 7-15　Windows 防火墙安全警报界面

很复杂。读者可以通过一些简单但是却很实用的入侵检测工具，建立起满足自己需求的基于网络、主机的入侵检测系统。下面以 Snort 系统为例，介绍入侵检测系统的安装和使用方法。

首先需要一台安装了 Windows XP 操作系统的计算机，并连接到本地局域网中。然后可以进行如下操作：

1. 安装并配置 Apache 服务器

(1) 到 Apache 官方网站上下载 Apache 的安装文件后，双击安装程序。选择“定制安装”，安装路径修改为 C:\apache 安装程序会自动建立 C:\apache2 目录，继续完成安装。

安装的时候注意本机的 80 端口是否被占用，如果被占用则关闭占用端口的程序。

(2) 添加 Apache 对 PHP 的支持。

具体步骤如下：

① 下载并解压缩 php-5.2.6-Win32.zip 安装包文件至 C:\php 目录下。

② 复制安装包中的 php5ts.dll 文件到 C:\windows\system32 目录下。

③ 复制 php.int-dist 文件到 C:\windows 路径下并重新命名为 php.ini。

④ 将 php.ini 打开，把“;extension=php_gd2.dll”和“;extension=php_mysql.dll”这两条语句前面的分号去掉。

⑤ 同时复制 C:\php\extension 下的 php_gd2.dll 与 php_mysql.dll 分别至 C:\windows 和 C:\windows\system32 下。

将 C: php\libmysql.dll 复制至 C:\windows\system32 下。

⑥ 添加 gd 库的支持，在 C:\apache\apache2\conf\httpd.conf 文件的末尾添加：

```
LoadModule php5_module "C:/php5/php5apache2.dll"
AddType application/x-httpd-php .php
```

⑦ 添加好后，保存 httpd.conf 文件，并重新启动 apache 服务器。

⑧ 测试 php 脚本：

首先在 C:\apache2\htdocs 目录下新建 test. php 文件，文件内容是：

```
<?phpinfo();?>
```

然后在 IE 浏览器中输入 http://localhost/test. php，测试 php 是否安装成功。

2. 安装并配置 Snort

(1) 下载并安装程序 WinPcap_4_0_2. exe；默认安装步骤即可。

(2) 下载并安装 Snort_2_8_1_Installer. exe；默认安装步骤即可。

(3) 将 snortrules\snapshot\current 目录下的所有文件复制(全选)到 C:\snort 目录下。

(4) 将文件压缩包中的 snort. conf 覆盖 C:\snort\etc\snort. conf。

(5) 在命令行方式下，进入 C:\ snort\bin，执行命令：

```
snort.exe -W
```

测试 Snort 是否成功安装。

3. 安装并配置 MySql

(1) 下载解压 mysql-5. 0. 51b-win32. zip 安装文件压缩包，并安装。

(2) 采取默认安装，记下设置的 root 账号和其密码。

(3) 检查是否已经启动 Mysql 服务：在安装目录 C:\mysql\bin 下运行命令：

```
mysql -u root -p
```

(4) 输入刚才设置的 root 密码。

(5) 继续运行以下命令：

```
c:\> mysql -D mysql -u root -p <  c:\snort_mysql
```

(6) 将 snort_mysql 复制到 C 盘下运行以下命令：

```
c:\mysql\bin\mysql -D snort -u root -p < c:\snort\schemas\create_mysql
c:\mysql\bin\mysql -D snort_archive -u root -p < c:\snort\schemas\create_mysql
```

这样就建立了 snort 运行必需的数据库。

4. 安装其他工具

(1) 安装 Adodb，解压缩 adodb497. zip 到 C:\php\adodb 目录下。

(2) 安装 jpgraph 库，解压缩 jpgraph-1. 22. 1. tar. gz 到 C:\php\jpgraph，并且修改 C:\php\jpgraph\src\jpgraph. php 文件，添加如下一行：

```
DEFINE("CACHE_DIR","/tmp/jpgraph_cache/");
```

(3) 安装 Acid，解压缩 acid-0. 9. 6b23. tar. gz 到 C:\apache\htdocs\acid 目录下，并将

C:\apache\htdocs\acid\acid_conf.php 文件的如下各行内容修改为：

```
$DBlib_path="C:\php\adodb";
$alert_dbname="snort";
$alert_host="localhost";
$alert_port="3306";
$alert_user="acid";
$alert_password="acid";
$archive_dbname="snort_archive";
$archive_host="localhost";
$archive_port="3306";
$archive_user="acid";
$archive_password="acid";
$ChartLib_path="C:\php\jpgraph\src";
```

(4) 通过 IE 浏览器访问 http:/127.0.0.1/acid/acid_db_setup.php，在打开的页面中单击“Create ACID AG”，让系统自动在 Mysql 中建立 Acid 运行必需的数据库。

5. 启动 Snort

(1) 测试 Snort 是否正常：

在命令行下输入以下命令：

```
C:\> snort -dev
```

能看到一只正在奔跑的小猪证明工作正常。

(2) 查看本地网络适配器编号：

在命令行下输入以下命令：

```
C:\> snort -W
```

查看本地网络适配器编号。

(3) 输入命令：

```
snort -c "C:\snort\etc\snort.conf" -i 2 -l "C:\snort\logs"-deX
```

“-i”后的参数为网卡编号，由“snort -W”察看得知，这时通过 IE 浏览器中输入 http://localhost/acid/acid_main.php 地址可以察看入侵检测的结果。

7.7.3 清除历史痕迹

在使用计算机的过程中，系统会将用户在计算机上的所有操作都记录下来，用户可以方便地查阅以前的操作。这些记录也会被黑客利用，为了保护计算机的安全，需要定期清理系统中保存的各种历史痕迹。使用 Windows 优化大师可以方便快速地清理系统中的历史痕迹，保护计算机的安全。

清除历史痕迹的方法步骤如下所述：

1. 下载与安装 Windows 优化大师

（1）访问 http://www.wopti.net/，进入下载中心，下载 Windows 优化大师安装文件。

（2）双击 Windows 优化大师安装文件图标 setup.exe Windows优化大师 共软网络，进入安装向导界面，如图 7-16 所示。

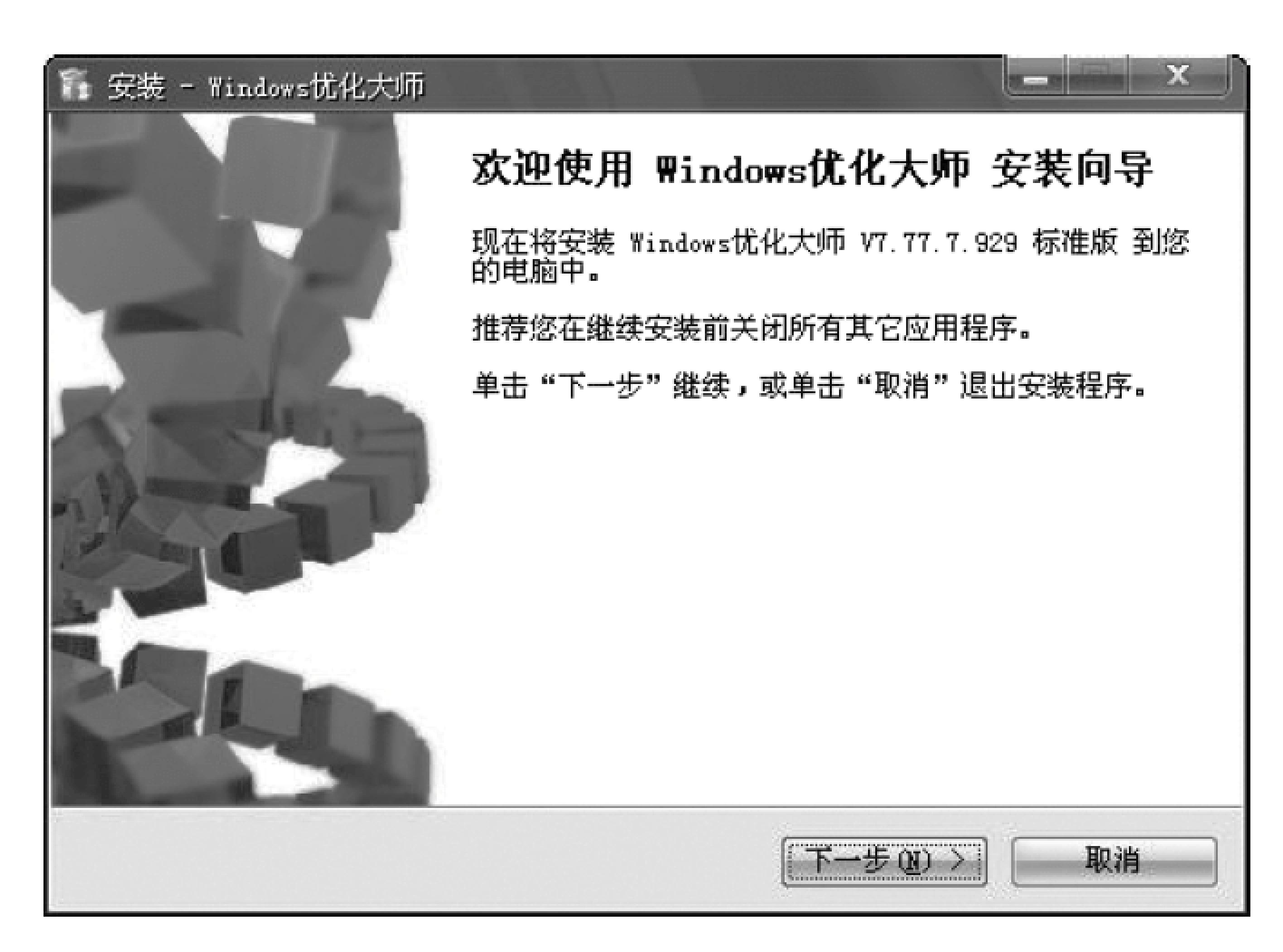


图 7-16　Windows 优化大师安装向导

（3）单击【下一步】按钮，出现“许可协议”介绍界面，如图 7-17 所示。选择“我同意此协议”，单击【下一步】按钮。

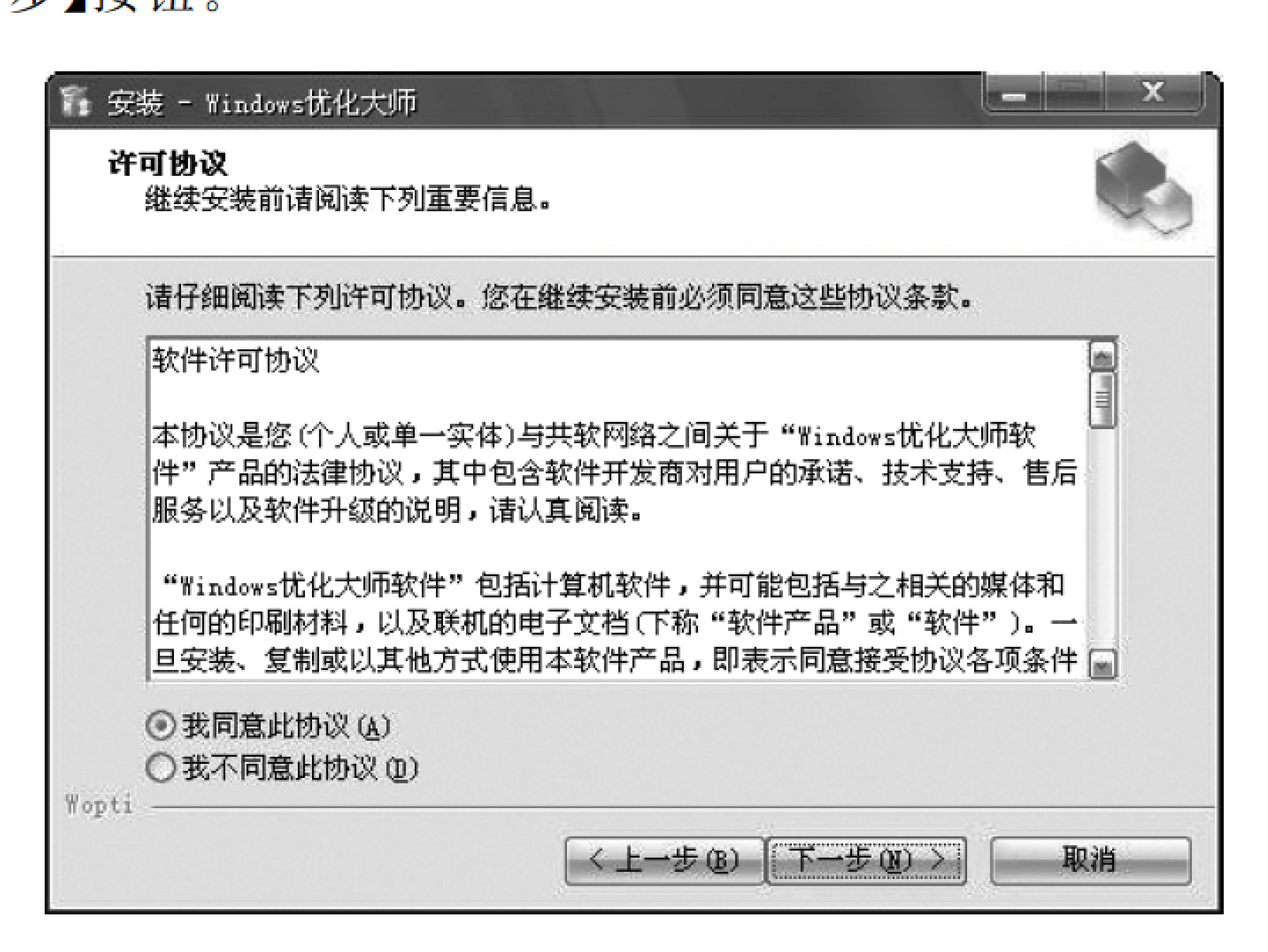


图 7-17　“许可协议”介绍界面

（4）选择软件安装位置，如图 7-18 所示，单击【下一步】按钮（Windows Vista 系统用户把软件安装至 C 盘以外的分区）。

（5）选择开始菜单中存放 Windows 优化大师的文件夹名，用户可以自己命名，也可存放在已有文件夹下。如果无须更改，直接单击【下一步】按钮，如图 7-19 所示。

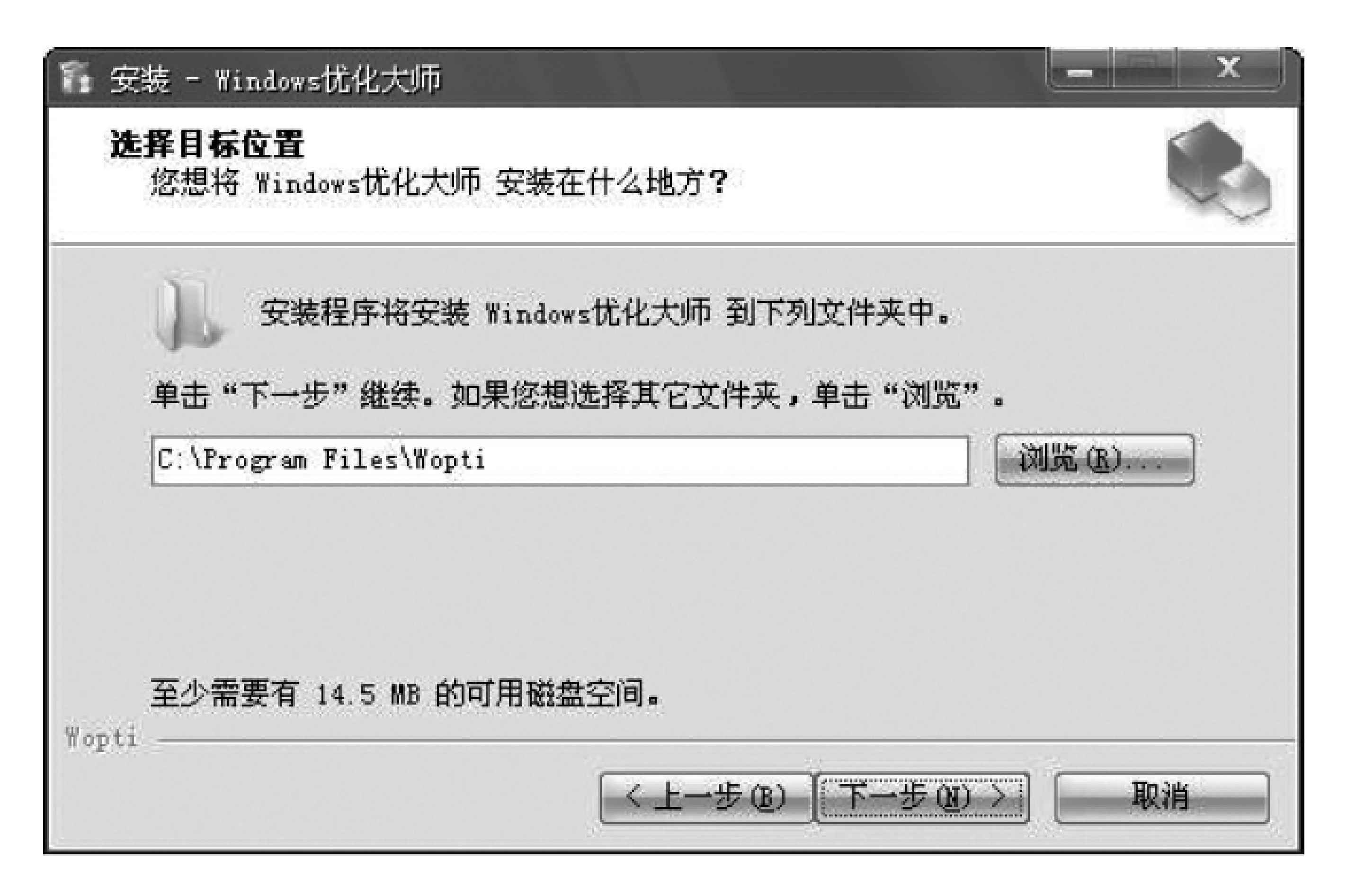


图 7-18 “选择目标位置”界面

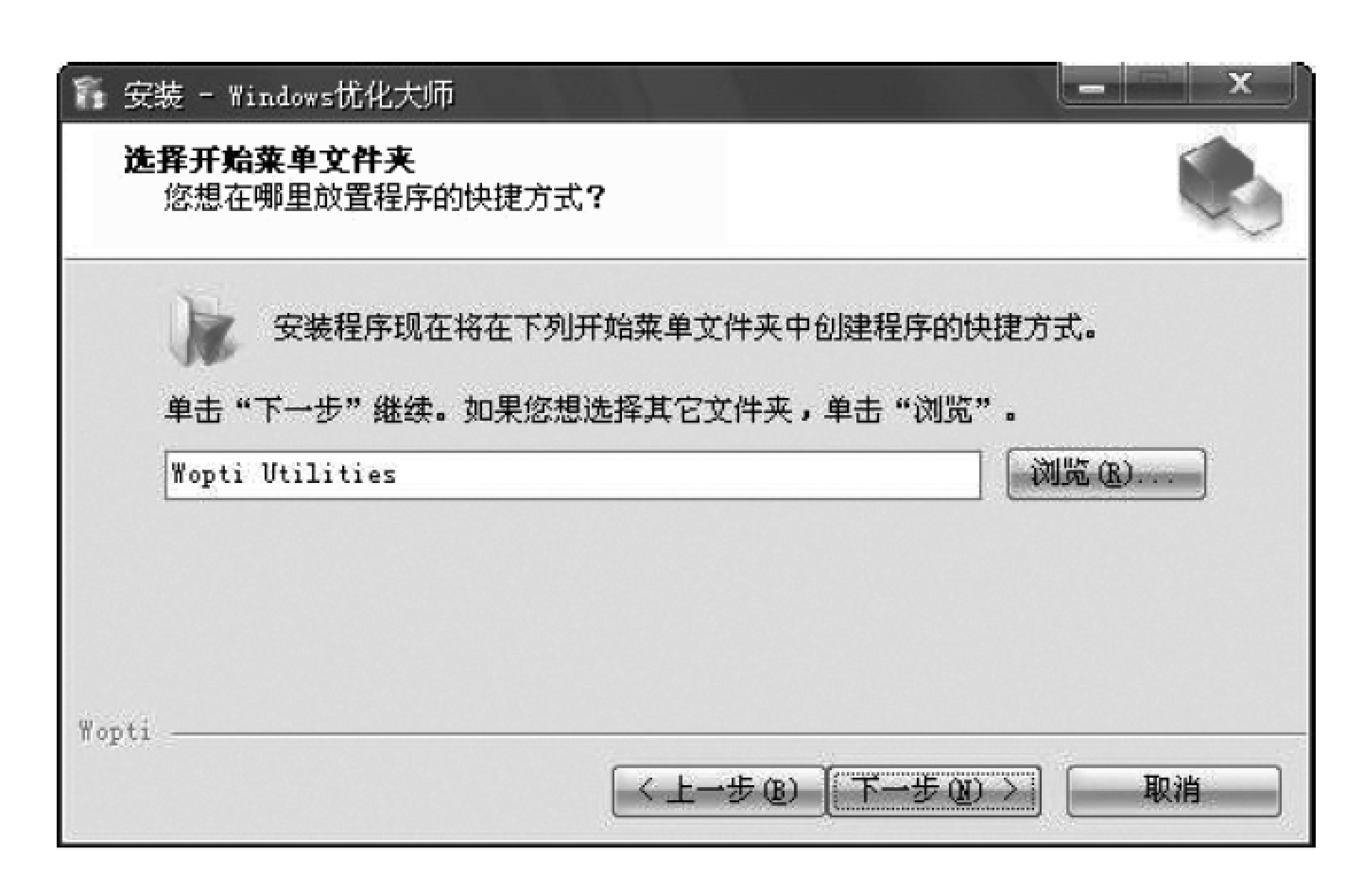


图 7-19 开始菜单快捷方式界面

(6) 默认“创建桌面快捷方式”,如图 7-20 所示,单击【下一步】按钮继续安装。

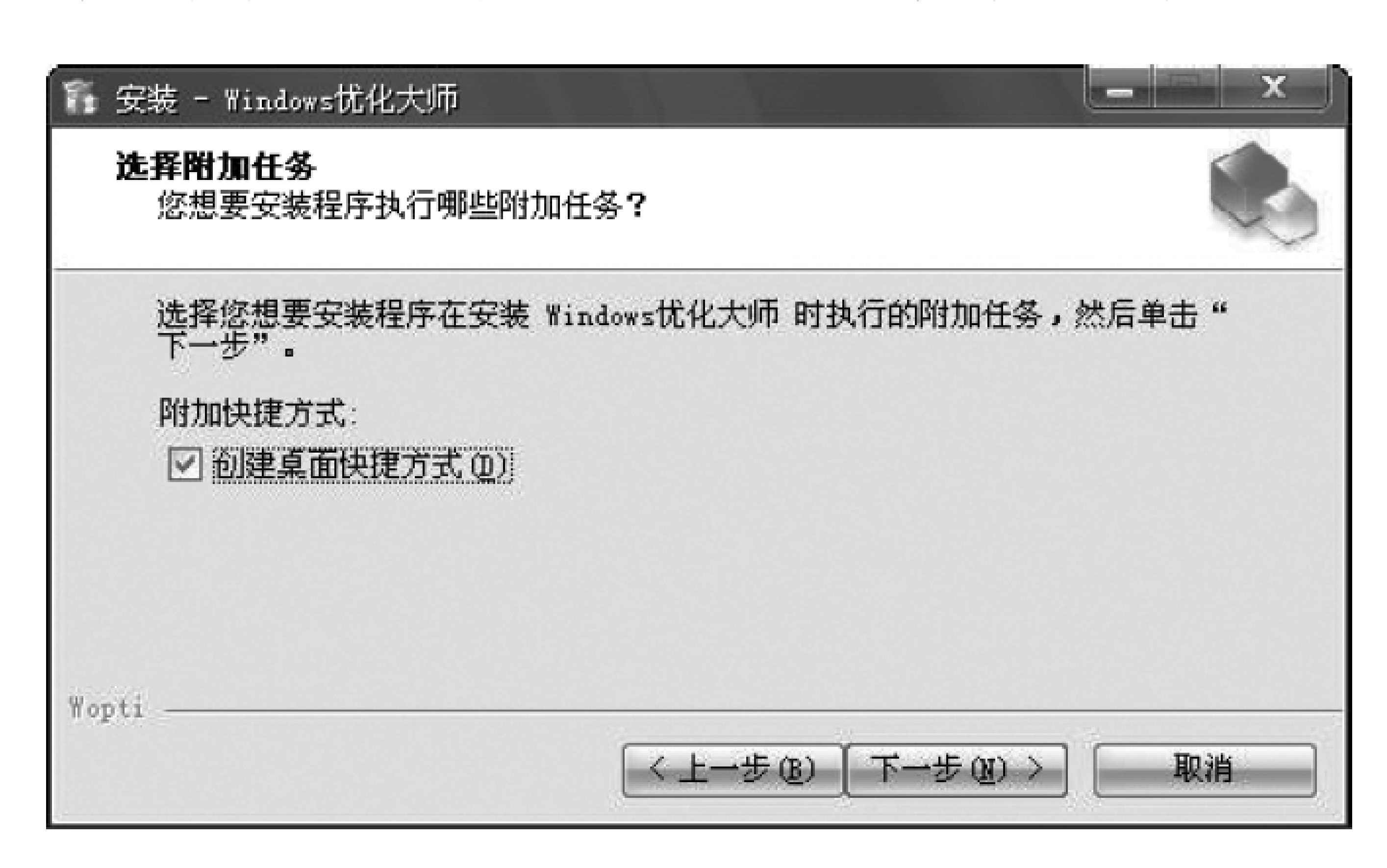


图 7-20 “创建桌面快捷方式”界面

(7) 确认无误后单击【安装】按钮,如图 7-21 所示。

(8) 安装成功后,勾选“运行 Windows 优化大师”选项,单击【完成】按钮,如图 7-22 所示。

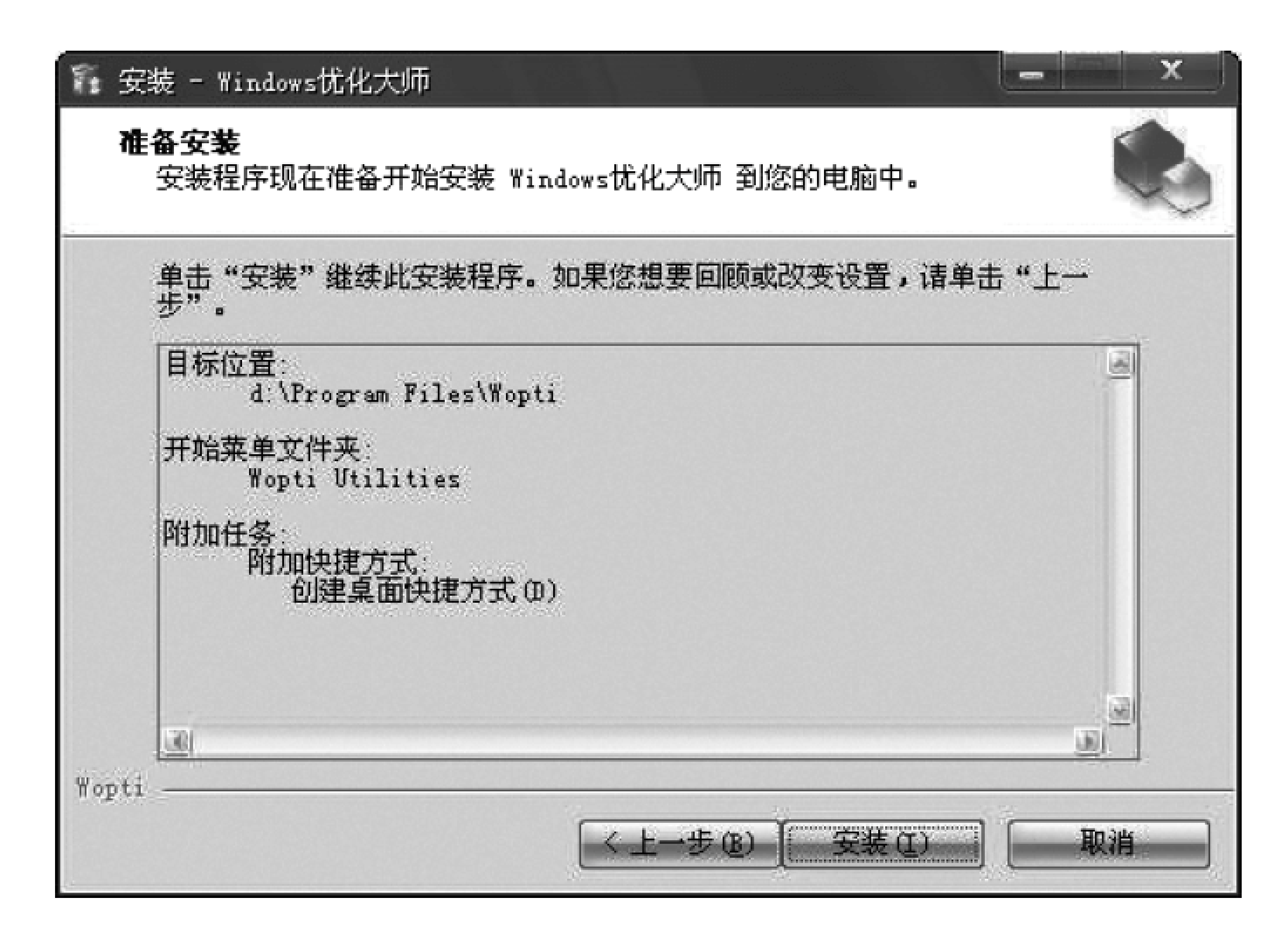


图 7-21 安装界面



图 7-22 安装完成界面

2. 使用 Windows 优化大师清理历史痕迹

第 1 步：双击桌面的“Windows 优化大师”快捷按钮，进入 Windows 优化大师界面。

第 2 步：单击界面左侧列表中的“系统清理”，可以看到四个功能，如图 7-23 所示。

第 3 步：单击图 7-23 界面左侧列表中的“历史痕迹清理”，进入历史痕迹清理界面，如图 7-24 所示。

图 7-24 中“请选择要扫描的项目”列表中包括了三个方面的内容：

(1) 网络历史痕迹。

① IE 缓存清理。用户可展开该节点，勾选需清理的内容。

② IE 地址栏中的历史记录。

勾选此项，将扫描 IE 浏览器地址栏中的 URL 历史记录。

注意：若用户习惯通过浏览器地址栏访问网站，请勿选择。



图 7-23　Windows 优化大师系统清理界面



图 7-24　历史痕迹清理界面

③ 清除表单和清除密码。

勾选这两项，将清除 IE 浏览器自动完成中的表单（例如：在搜索引擎中输入的曾经搜索过的字符串）和密码历史记录。

注意：若用户习惯浏览器保存您的表单或密码，请勿选择。

（2）Windows 使用痕迹。

此大类下，包括了运行对话框历史记录、窗口位置与大小历史记录等 Windows 产生的历史痕迹。本大类下的条目通常可以勾选。

由于 Windows 使用痕迹随用户使用计算机而不断产生，故建议用户不定期清理（例如：每月一次）即可。

（3）应用软件历史记录。

此大类下，包括了 Media Player、RealPlayer 等应用软件使用过程中生成的历史记录。

第 4 步：用户根据自己的实际情况勾选相应选项，然后单击【扫描】按钮，如图 7-25 所示。



图 7-25　扫描结果

第 5 步：观察扫描结果列表，单击【全部删除】按钮，或者根据需要勾选相应的文件，然后单击【删除】按钮。

以上操作完成后，用户在系统中留下的使用痕迹就被消除了。

7.8　案例讨论

2011 年 5 月 1 日，索尼公司表示，黑客可能已窃取了该公司旗下索尼在线娱乐 PC 游戏网络中的超过 2500 万个账户信息。

此前一天，索尼刚刚宣布将采取措施应对类似两周前 PlayStation Network（以下简

称“PSN”)遭遇的攻击。根据索尼的说法,索尼在线娱乐 PC 游戏网络于 4 月 18 日遭到攻击,但索尼直到 4 月 20 日才发现用户数据失窃。索尼随后很快关闭了这一服务。在此次事件中,奥地利、德国、荷兰和西班牙的 10 700 个直接付款记录可能被泄露,而 12 700 个非美国信用卡或贷记卡号码也可能失窃。到目前为止,索尼旗下大约九个服务网站因最初的泄密事件而被黑客攻破。

2011 年 7 月 29 日,韩国通信委员会声称,黑客袭击了韩国一家门户网站和一家博客网站,涉及高达 3500 万名用户的个人信息。这可能是韩国迄今为止遭到的最大网络攻击案。有报道称,韩国门户网站 Nate 和博客网站赛我网(Cyworld)遭黑客攻击,两家网站用户数量分别为 2500 万和 3300 万人,约有 3500 万名用户的信息外泄。

根据得到核实的受损情况,被泄露的信息包括未经加密的用户名、用户姓名、电话号码、电子邮件和经加密的密码、身份证号码等。韩媒称,由于用户姓名和电话号码大量被泄露,有可能出现利用这些个人信息的电话诈骗、发送垃圾邮件等非法行为。

2011 年 12 月 21 日,中国开发者技术在线社区 CSDN 遭黑客攻击,600 万用户账户密码被黑客在网上公布。CSDN 对此公开致歉,并提醒用户修改密码。此外,据传包括多玩、178 游戏网、U9、7k7k 等业内多家网站也被黑客攻击,导致账号外泄,涉及用户资料在 5000 万以上。由此引发了大众对隐私安全的关注,2011 年成为黑客行动主义进入主流的一年。面临黑客如此猖獗的攻击活动,网络安全形势非常严峻。

可以看出,网络攻击威胁到每个人、每个企业、每个国家的网络安全。你认为,一个网络遭受网络攻击,是否仅仅在于防御技术的缺陷呢?

你是否注册过 CSDN 用户?该公司用户信息泄露对你产生了什么影响?

归纳总结

1. 通过本章内容,归纳总结有哪些网络攻击手段。

2. 归纳总结企业级计算机信息系统有可能遭受哪些网络攻击与入侵,总结作为企业级信息系统需要掌握哪些网络攻击防御技术。

3. 归纳个人计算机有可能遭受哪些网络攻击与入侵,总结作为个人需要掌握哪些网络攻击防御技术。

思考与实践

思考题

1. 什么是网络攻击?什么是网络入侵?二者有什么关系?
2. 你如何看待黑客呢?
3. 按照攻击者的目的可以把网络入侵与攻击分为哪些类型?
4. 扫描的目的是什么?包含哪些类型?
5. 蜜罐技术有什么作用?

6．防火墙的基本体系结构有哪几种？各有什么优缺点？

实践题

1．归纳总结你曾遇到过的网络攻击与入侵行为，以及这些行为造成了什么样的危害。

2．使用某种扫描软件，查看一台主机，说明该主机运行的是什么操作系统，提供了哪些服务，有什么漏洞。

3．下载一款个人防火墙，熟悉其功能和操作，并根据自己的需要设置防火墙，并评估其优缺点。



第8章 网络应用安全技术

学习目标

通过本章的学习，能够——

- 了解网络应用安全面临的威胁；
- 知道网络应用的常用安全措施；
- 了解网络应用安全技术的作用；
- 掌握360木马防火墙的使用方法。

引导案例

2011年末，中国互联网用户遭遇了一场最大规模的个人信息泄露事件，而此次“泄密门”事件波及的范围有互联网科技公司，互联网电商企业，甚至连银行、出入境管理局登记数据也被传有泄露。最早陷入此次“泄密门”事件的是CSDN公司。12月21日，有黑客在网上公开了CSDN网站用户数据库，600万注册邮箱账号和密码被公布到了互联网上。12月22日起，网上先后曝出人人网、开心网、多玩、天涯等知名网站的用户注册信息。据不完全统计，网上泄露出来的各类用户信息，可能已经超过一亿个。互联网行业一片人心惶惶，12月29日下午，在用户数据最为重要的电商领域，也不断传出存在漏洞、用户泄露的消息，漏洞报告平台乌云发布漏洞报告称，支付宝用户大量泄露，被用于网络营销，泄露总量达1500万～2500万之多，泄露时间不明，里面只有支付用户的账号，没有密码。此外，被卷入的企业还有京东商城、支付宝和当当网。

2012年1月9日，“CSDN泄密门”事件传出最新消息，两名涉案黑客已经被抓，还有部分人员尚未落网。

针对大规模的密码泄露事件，工信部于2011.12.28日发布通告，强烈谴责窃取和泄露用户信息的行为，同时要求各互联网站要及时发现和修复安全漏洞。工信部还提醒广大互联网用户提高信息安全意识，密切关注相关网站发布的公告，并根据网站安全提示修改密码，提高密码的安全强度并定期修改。

8.1　网络应用安全概述

本节主要介绍网络应用安全的概念，网络应用安全存在的威胁以及应对措施。

8.1.1　网络应用安全的概念

1. 网络应用的定义

网络应用是依托网络通过信息系统为用户提供服务及开展公司的业务工作。网络应用直接与成千上万的用户打交道，用户通过网络应用可以进行网上冲浪、搜索信息、网上购物、下载文件、看电视、发短信、聊天等。

网络应用服务是在网络上利用软/硬件平台满足特定信息传递和处理需求的行为，即在网络上由网络服务供应商开放的一些服务，常见的如 Web、E-mail、FTP、DNS、Talent 等，当然也有一些非通用的、在某些领域和行业中自主开发的网络应用服务，如办公自动化、电子商务与电子政务、远程教育等。

2. 网络应用安全的定义

网络应用安全可理解为网络应用服务的安全，指的是主机上运行的网络应用服务是否能够稳定、持续运行，不会受到非法的数据破坏及运行影响。它的要求是要保证网络用户的真实性，互联网数据传输的机密性、完整性和可靠性，以便对抗身份假冒、信息窃取、数据篡改、越权访问和事后否认等安全威胁。其目标有：

（1）保护网络系统中存储和传输信息的保密性和完全性。

（2）保护网络系统的可用性。

（3）保护网络系统服务的可靠性。

（4）保证网络资源访问的可控性（防范非法访问及非授权访问）。

（5）防范入侵者的恶意攻击与破坏。

（6）防范病毒的侵害。

（7）实现网络的安全管理。

8.1.2　网络应用安全存在的威胁

根据网络应用安全的概念，可以从以下几个方面来分析网络应用安全中存在的威胁：

1. 非授权访问

非授权访问是指没有预先经过同意就使用网络或计算机资源，如有意避开系统访问控制机制对网络设备及资源进行非正常使用，或擅自扩大权限越权访问信息。例如黑客通过破解口令得到用户某些账号，这些账号可能是用户的网上银行账号，网络游戏账号等，从而假冒合法用户进入网络系统进行违法操作，或者某些系统管理员以未授权方式进行某些操作，从而造成危害。

2. 信息泄露或丢失

信息泄露是指敏感数据或重要数据在有意或无意中被泄露出去或丢失，它通常包括信息在传输中丢失或泄露、信息在存储介质中丢失或泄露、通过建立隐蔽隧道等窃取敏感或重要信息等。例如网络用户在使用网上银行进行网上支付时可能受到黑客攻击，从而造成个人信息泄露或丢失。

3. 破坏数据完整性

以非法手段窃得对数据的使用权，如删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。例如电子邮件在因特网传输的过程中，攻击者在电子邮件数据包经过这些邮件服务器的时候把它截取下来，获得这些邮件的信息，删除某些数据包后重新将邮件发送出去，从而造成了数据的不完整。

4. 拒绝服务攻击

拒绝服务攻击就是用某种方法耗尽网络设备、链路或服务器资源，使其不能正常提供服务的一种攻击手法。目前常见的拒绝服务攻击主要有利用操作系统或应用程序漏洞使服务器崩溃；通过发送大量垃圾信息浪费链路带宽，使正常信息因为阻塞而被丢弃。例如攻击者使用垃圾邮件，邮件炸弹或者对 QQ 进行轰炸等，使网络资源大量消耗，从而造成被攻击者网站网路堵塞，使大量的用户不能正常使用邮件和 QQ。

此外，网络应用安全威胁还有网络钓鱼和“肉鸡”，网络钓鱼是指攻击者利用伪造的 Web 站点和欺骗性的电子邮件来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容，其典型特点是具有欺骗性、针对性、手段的多样性、隐藏性和潜在性。“肉鸡”是指被黑客攻破，种植了木马病毒，从而被黑客控制的计算机。

8.1.3 网络应用安全的防范措施

针对以上网络应用安全中存在的威胁，可以从以下几个方面进行防范：

1. 使用防火墙技术

防火墙技术是目前保障网络安全所普遍采用的安全技术，它可以实现对网络的访问控制，保护内部网络不遭受外部网络（互联网）的攻击和非法访问。

2. 使用入侵防御系统，进行主动安全防御

入侵防御系统（IDS）属于主动安全技术，它能实现实时监控、检测和分析数据流量，并能深度感知和判断哪些报文是恶意的报文，能通过对恶意报文进行丢弃以阻断攻击。IDS 只能检测网络攻击行为并告警，但产品自身无法阻止网络攻击行为。

3. 采用加密技术和数字证书保证信息安全

加密技术是指通过对网络中传输的信息进行加密来保障其安全性,是一种主动的安全防御策略。数字证书是指一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。通过两者结合,可以提高网络数据的安全性,并实现用户的身份认证。目前主要用于网上银行与网上支付,保证银行用户的个人信息安全和支付安全。

4. 其他相关的安全措施

针对不同的网络应用安全威胁,应该采用不同的安全措施。例如对于口令攻击,应该设置安全的口令,来保护口令安全;对于垃圾邮件和邮件炸弹,可以安装垃圾邮件清除软件和炸弹清理软件进行邮件过滤;对于文件传输可以采取限制端口和对服务器端软件进行安全设置;对于网络钓鱼可以采用网络防钓鱼技术和用户提高个人安全意识等措施进行防范。对于肉鸡可以采用相应的防肉鸡技术。

8.2 常见网络应用的安全措施

本节从口令的安全入手,结合 E-mail、QQ、网上购物、网上银行等常用的网络应用服务在提供服务的过程中出现的安全问题,提出相应的安全措施,希望为读者提供一些实用的应用安全措施。

8.2.1 口令的安全

口令认证是目前防止非法者进入和使用系统最有效、最常用的做法之一。获取合法用户的账号和口令已经成为黑客攻击的重要手段之一。在有些情况下,黑客必须取得合法用户或管理员的口令以此进入并控制系统。现在,有一部分人喜欢破解他人的各种口令,如 E-mail,基于 Web 的访问口令,网络游戏的账号等,这也给网络安全造成一定的威胁。

1. 口令的破解方式

分布式破解法(distributed cracking)是破解口令的一种方式。分布式破解法就是入侵者用独立的几个进程,并行地执行破解工作,其实现有几种方法,其中之一就是将口令文件分解成几块,在各自独立的计算机上分别破解这几块文件。通过这种方法,破解工作被分散到不同工作站上进行,花费的时间和资源就少了。

分布式破解法的问题是它会带来许多麻烦,不分散 CPU 负载,另一方面是系统管理员很容易注意到自己的大量处理器资源被消耗,注意到有一个进程已经运行了一天多。因此,对于入侵者来说,分布式破解法并不可行,除非他们是一个站点的管理员或有自己的网络。

2. 口令的破解机制

口令破解机制有两种方法：①字表被送到加密进程加密，通常是一次加密一个单词。加密过程中使用了各种规则，每加密一个单词，就把它与目标口令(同样是加密的)对比，如果不匹配，就开始处理下一个单词。②口令入侵者的执行过程与此不同，它们取出整个字表，应用一条规则进行加密，从而生成下一个字表，再对这个字表进行加密，再与目标口令匹配。这两种方法没有实质性的区别，只是第二种方法可能更快些。

最后如果有一个单词与目标口令匹配，则认为口令被破解，相应的明码正文单词被存入文件(记录在明码正文文件中，留待后面检查)。

3. 常见的口令攻击方式

基于 Internet 的口令攻击模型如图 8-1 所示，口令认证的过程是用户在本地输入 ID 和口令，经传输线路到达远端系统进行认证。由此，就产生了 3 种口令攻击方式，即从用户主机中获取口令，在通信线路上截获口令，从远端系统中破解口令。

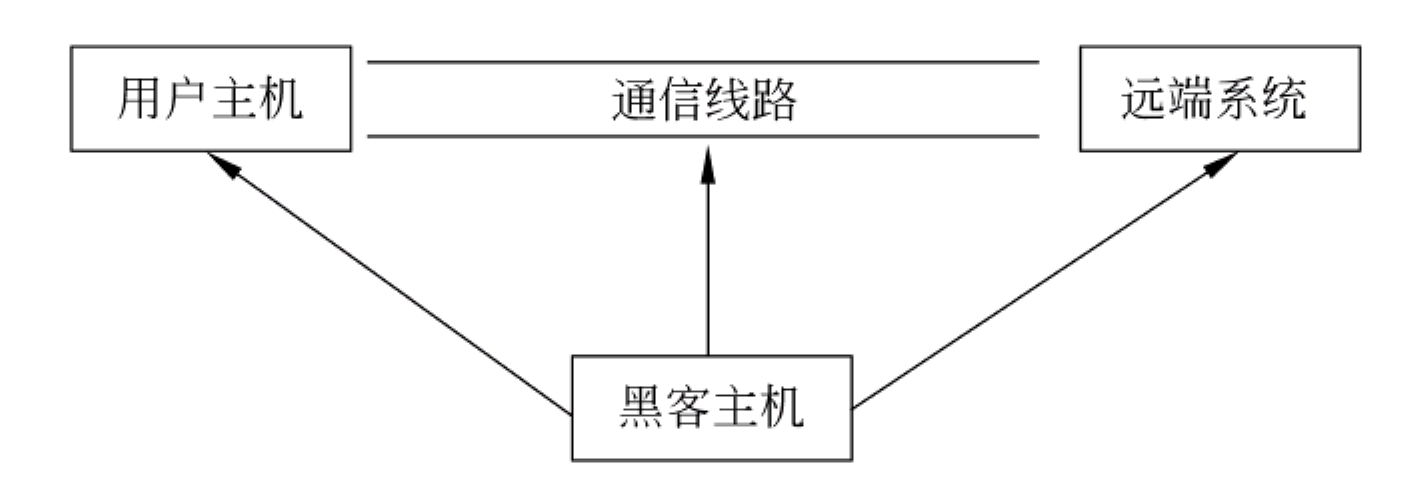


图 8-1　基于 Internet 的口令攻击模型

(1) 从用户主机中获取口令。

攻击者对用户主机的使用权限一般可分为两种情况：一是具有使用主机的一般权限；二是不具有使用主机的任何权限。前者多见于一些特定场合，如企业内部。大学校园的计算中心、机房等。所要破解的密码有 Word、Excel、Power Point、Access 等一些办公文件密码等。所使用的工具多为可从网上下载的专用软件。这对于攻击者来说不需要有太高的技术水平，只要能使用某些软件就可以进行破解。对于后者一般要与一些黑客技术配合使用，如特洛伊木马、后门程序等。这样可使攻击者非法获得对用户计算机的完全控制权，然后再在目标主机上安装木马、键盘记录器等工具软件来窃取被攻击主机用户输入的口令字符串。

(2) 在通信线路上截获口令。

现在，公司、大学或者网吧都建有自己的局域网，局域网通过网络互联设备与外部的 Internet 相连。由于局域网的特殊结构，使得黑客可以利用嗅探器截取在通信线路上传输的口令信息。

嗅探器是一种利用计算机网络接口截获其他计算机的数据报文的程序。在合理的网络中，嗅探器的存在对于系统管理员来说是很重要的，但若为某些人所使用，却可以造成用户口令的泄露。

（3）从远端系统中破解口令。

所谓远端系统是指 Web 服务器或攻击者要入侵的其他服务器。破解的口令有 Telnet、FTP，基于 Web 的访问口令，系统中一般用户和管理员的口令等。

黑客入侵系统时，常常把破译系统中普通用户口令作为攻击的开始，因为只要取得系统中一般的访问权限，就很容易利用系统的本地漏洞来取得系统的控制权。在线或离线攻击是 Internet 上常用的口令攻击手段。攻击者在在线或离线状态下，对用户口令进行穷举或字典法猜测攻击。穷举法是对纯数字的密码有很好的破解效果，但若密码中含有字母或其他字符就不适合采用这种方式。它的原理是逐一尝试数字的所有排列组合，直到破解出密码或尝试完所有组合为止。字典法是指由于某些用户喜欢使用英文单词，姓名拼音、生日、数字或这些字符的简单组合作为密码。黑客就可以先建立包含大量此类单词的密码字典，然后使用程序一一尝试字典中的每个单词，直到破解出密码或字典被遍历为止。

4. 安全口令的设置

针对口令使用中存在的安全问题，作为普通的口令用户，应该从以下几个方面设置安全的口令，防止口令被盗。

（1）避免设置弱口令。

弱口令是指容易被破解的口令。从理论上讲，没有破解不了的口令，但精心设置的口令，能大大增加破解的难度。如果破解所需的时间成本远大于破解后的可能回报，黑客就会认为得不偿失.主动放弃破解。因此，只有强口令才具有安全防范作用。

（2）设置口令时要避免的一些错误做法。

设置口令时要避免的错误做法主要包括：使用空口令，使用默认口令，使用账号作为口令，多处登录用同一个口令，用个人信息作口令，使用短口令或纯字母、纯数字口令，长期使用一个口令，将口令写入硬盘文件中，登录时让系统记下口令。

（3）设置安全口令的技巧。

最好的口令用户很容易记住，但黑客却很难猜到或破解。强口令的设置起码应符合以下要求：

① 口令长度至少要 8 位以上。根据国家保密规定，处理秘密级信息的系统口令长度不得少于 8 位，机密级的不得少于 10 位。

② 口令中综合使用各种符号。键盘上的大小写字母、数字和其他符号共计有 96 个，用它们排列组合形成的口令强度大，普通计算机破解 8 位这样的口令大致需要 23 年。

③ 经常更换口令。根据国家保密规定，处理秘密级信息的系统口令的更换周期不得长于 30 天，机密级的是 7 天，绝密级的则应当采取一次性口令。

要得到好记的强口令，可以使用密码短语法。首先选取一句你喜欢的且容易记住的话，如诗词、名言警句、歌词、口头禅等，然后取其拼音的第一个字母，连起来就组成一个口令。例如：“天上的星星数呀数不清”这句童谣，其拼音的首字母连起来得到 tsdxxsysbq。第二步是进行个性化改造。利用音似和形似的原理变化调整口令，如可将上述口令中的 xx 变为 * *，将最后的 q 字母变为数字 9，将第一个字母大写，最后得到 Tsd * * sysb9。

运用类似这样的方法，甚至可以借鉴学习当前在青少年网民中流行的“火星文”。充分发挥你的想象力，就能得到让黑客伤透脑筋但又让自己轻松记住的口令。

8.2.2 E-mail 的安全

电子邮件已成为人们日常生活中重要的联系方式之一，在很大程度上取代了传统的信件邮寄。但是电子邮件并不像密封邮寄，在到达目的地之前不知道经过了多少节点。因此电子邮件系统已受到机密泄露、信息欺骗、病毒侵扰等许多安全问题的困扰。确保电子邮件的安全使用也越来越迫切。

1. E-mail 的工作原理

电子邮件与普通邮件有类似的地方，发信者注明收件人的姓名与地址(即邮件地址)。发送方服务器把邮件传到收件方服务器，收件方服务器再把邮件发到收件人的邮箱中。其工作原理图如图 8-2 所示：

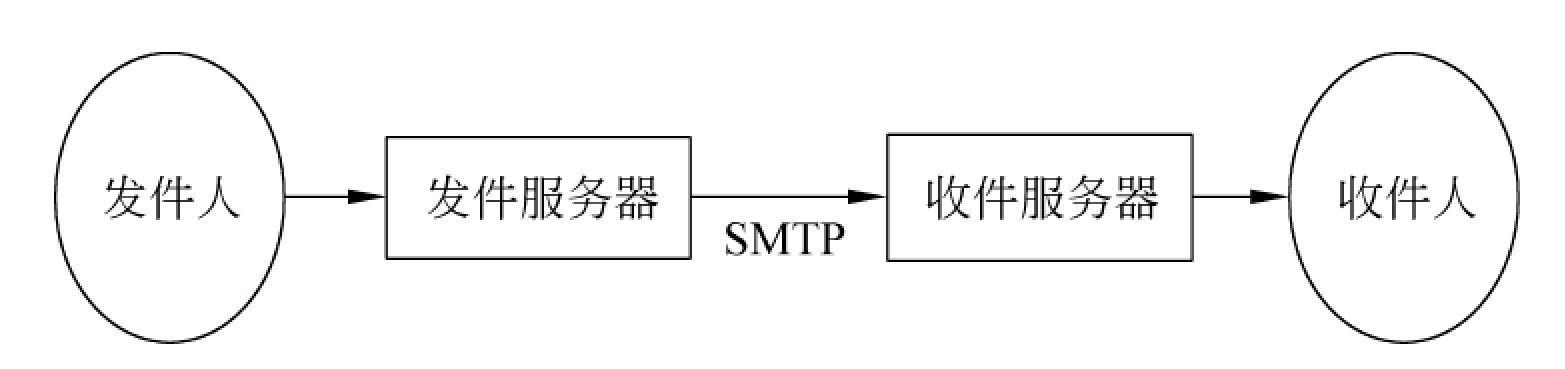


图 8-2 电子邮件的工作原理

电子邮件的工作过程是：电子邮件由发信方编辑，通过客户端程序将编辑好了的电子邮件向 SMTP 服务器发送，SMTP 服务器识别到收信人的地址，并向管理该地址的 POP3 服务器发送消息，邮件服务器识别后将消息存放在接收者的电子信箱内，并告知收信人有新邮件到来。收信人通过邮件客户程序连接到服务器后，就会看到服务器的通知，进而打开自己的电子信箱来查收邮件。

2. E-mail 的安全漏洞与威胁

基于前述电子邮件的工作原理，目前电子邮件主要有以下的安全漏洞与威胁：

(1) SMTP 的安全漏洞。

电子邮件在因特网传输时，一般采用 SMTP，其属于 TCP/IP 的协议，该协议明确定义了计算机系统间电子邮件的交换规则。邮件在发送时需要用不同的邮件服务器进行转发，这种转发过程一直持续到电子邮件到达最终接收主机。而 SMTP 自身存在先天安全隐患，它传输的数据没有经过任何加密，于是攻击者在电子邮件数据包经过这些邮件服务器的时候把它截取下来，就可获得这些邮件的信息，然后按照数据包的顺序重新还原成你发送的原始文件。邮件发送者发送完电子邮件后，不知道它会通过哪些邮件服务器到达最终的主机，也无法确定在经过这些邮件服务器时是否有人把它截获下来。从技术上看，没有任何办法可以阻止攻击者截获在网络上传输的数据包。

(2) 电子邮件接收客户端软件的安全漏洞。

邮件接收客户端软件的设计缺陷也会造成电子邮件的安全漏洞，如微软的 Outlook

和 Outlook Express 功能强大，能够和操作系统融为一体，具有相当多的使用者，但它们可能传播病毒和木马程序。一旦木马程序进入用户计算机，一切都将会处于黑客的控制之下。而病毒一旦发作，轻则损坏硬盘上的文件，甚至整个硬盘，重则会造成整个网络的瘫痪。

电子邮件传播病毒通常是把自己作为附件发送给被攻击者，一旦被攻击者打开了病毒邮件的附件，病毒就会感染其计算机，然后自动打开其 Outlook 的地址簿，将自己发送到被攻击者地址簿上的每一个电子邮箱中，这正是电子邮件病毒能够迅速大面积传播的原因所在。电子邮件客户端程序的一些 bug 也常被攻击者利用来传播电子邮件病毒。Outlook 曾经就因为存在这方面的漏洞被攻击者用来编制特殊的代码，这样，即使被攻击者收到邮件后不打开附件，也会自动运行病毒文件。

（3）垃圾邮件。

垃圾邮件是指向新闻组或他人电子邮箱发送的未经用户准许、不受用户欢迎的、难以退掉的电子邮件或电子邮件列表。垃圾邮件的常见内容包括商业或个人网站广告、赚钱信息、成人广告、电子杂志等。垃圾邮件可以说是因特网给人类带来的副产品：其一，占用网络带宽，造成邮件服务器拥塞，降低了整个网络运行的速率。其二，侵犯收件人的隐私权，耗费收件人的时间、精力和金钱，占用收件人信箱空间。其三，严重影响 ISP（Internet 服务提供者）的形象。在国际上，频繁转发垃圾邮件的主机会被上级因特网服务提供商列入垃圾邮件数据库，从而导致该主机不能访问国外许多网络。而且收到垃圾邮件的用户会因为 ISP 没有建立完善的垃圾邮件过滤机制，而转向其他 ISP。其四，骗人钱财，传播色情，发布反动言论等内容的垃圾邮件，已经对现实社会造成危害。其五，被黑客利用成为助纣为虐的工具。如 2000 年 2 月，黑客攻击雅虎等 5 大热门网站时，先是侵入并控制了一些高带宽的网站，集中众多服务器的带宽能力，然后用数以亿万计的垃圾邮件猛烈袭击目标，造成被攻击者网站网路堵塞，最终瘫痪。

（4）邮件炸弹。

邮件炸弹是指邮件发送者通过发送巨大的垃圾邮件使对方电子邮件服务器空间溢出，从而造成无法接收电子邮件，或者利用特殊的电子邮件软件在很短的时间内连续不断地将邮件发送给同一个信箱，在这些数以千万计的大容量信件面前，收件箱不堪重负，最终“爆炸身亡”。信箱被撑满后，如果不及时清理，将导致所有发给该用户的电子邮件被主机退回。而被撑爆的信箱很可能会一直出错，从而导致其信箱长时间处于瘫痪状态。邮件炸弹还会大量消耗网络资源，常常导致网络塞车，使大量的用户不能正常使用。

3. E-mail 的安全防范措施

作为电子邮件提供商，应该对电子邮件用户的邮件进行加密，保护电子邮件的内容安全。其具体方法是在发送邮件前对其进行数字加密处理，接收方接到电子邮件后对其进行数字解密处理，这样，即使攻击者截获了电子邮件，他面对的也只是一堆没有任何意义的乱码。所谓加密，是指将一个明文信息经过加密密钥及加密函数的转换，变成无意义的密文，当需要的时候则将此密文经过解密函数、解密密钥还原成明文。最常用的加密软件是 PGP（Pretty Good Pfi-vaey），PGP 是一个基于公钥加密体系（rivest shamir adleman，

RSA)的邮件加密软件，它提出了公共钥匙或不对称文件加密和数字签名。多数用户的邮件在Internet上传输时不采取任何安全措施，没有安全措施的邮件很容易被别有用心者盗用，从事非法活动。如果用户将电子邮件错发给陌生人，收信人也有可能利用错发的明文邮件做文章。采用数据加密和数字签名可以保护电子邮件的内容安全。

作为普通的电子邮件用户，应该从以下两个方面对电子邮件进行安全防范：

(1) 对邮件和系统进行病毒防护。

首先选择一款可靠的防毒软件，目前常用的防毒软件有瑞星、KV3000、KILL、金山毒霸、诺顿等，用户可打开防毒软件的电子邮件扫描功能，对来往邮件的病毒进行拦截，可有效防止邮件病毒的侵入，并防止将感染病毒的电子邮件发送给其他用户。同时，及时升级病毒库，随时补充新病毒代码到病毒库中。然后打开实时监控防火墙，实时监控技术为电子邮件和系统安全构筑起一道动态、实时的反病毒防线，它通过修改操作系统，使操作系统本身具备反病毒功能，拒病毒于计算机系统之门外。再次，识别邮件病毒并学会处理，当收到邮件时，先看邮件大小及对方地址，如果发现邮件中无内容，无附件，邮件自身的大小又有几十KB或更大或者附件的后缀名是双后缀，那么此类邮件中极可能包含病毒，可直接删除此类邮件，然后再清空垃圾箱。在清空垃圾箱后，一定要压缩一遍邮箱，否则杀毒软件在下一次查毒时还会报有病毒。此外，还可以通过少使用信纸模块，设置邮箱自动过滤功能，不使用邮件软件中的预览功能对病毒进行防范。

(2) 对垃圾邮件和邮件炸弹进行过滤。

对于垃圾邮件和邮件炸弹最好使用垃圾邮件清除软件和炸弹清理软件进行过滤、自动删除，它们可以为用户提供方便而强大的保护。常用的清除软件有Spamkiller(垃圾邮件杀手)、SpamEater Pro(垃圾邮件吞食者)、SpamAttack Pro(垃圾邮件终结者)，BombCleaner等炸弹清理软件，在不接收信件的时候查看邮件清单，从中选择垃圾信件进行远程删除，这样既节约了大量下载信件的时间，同时也堵住了通过电子邮件传播的病毒。此外，不要随便公开自己的邮箱地址，设置邮件的大小，设置邮箱过滤都可以防范垃圾邮件和邮件炸弹。

8.2.3 QQ的安全

1. 常见的QQ安全问题

(1) QQ漏洞。

QQ漏洞主要有程序漏洞、业务漏洞、后台服务漏洞、游戏漏洞等。QQ程序漏洞是指聊天软件本身存在的各种漏洞，黑客利用这些漏洞可以在使用QQ聊天的过程中散发携带恶意代码的网址和程序脚本等，还可以利用程序漏洞对聊天对象发动信息Flood攻击和IP攻击等。业务漏洞主要是指在QQ服务中存在的漏洞，通过QQ业务漏洞，黑客可以非法获得大量的Q币，可以在QQ游戏、QQ空间、QQ邮箱等服务的内容中获取利益。后台服务漏洞指QQ程序在后台支持服务过程中存在的漏洞，此类漏洞可能妨碍QQ程序的正常服务。游戏漏洞是在QQ游戏中存在的漏洞，黑客通过这些漏洞可以刷Q币，刷积分甚至窃取QQ号码，从而谋求利益。

(2) QQ 密码被盗。

QQ 密码被盗的主要原因有密码设置过于简单,登记在 QQ 里的 E-mail 账户被黑,使用的计算机中了木马程序。

(3) QQ 聊天记录被泄。

QQ 的聊天记录可以被偷窥是因为一个可以绕过密码在本地登录的漏洞。当用户在系统登录 QQ 以后,就会在 QQ 安装目录生成一个该 QQ 号码的文件夹,里面保存了该号码所有的配置信息、聊天记录等。通过这个漏洞黑客可以绕过远程系统的密码验证,从而突破 QQ 程序本身的限制,获取记录在本地的信息内容。

(4) QQ 被炸。

QQ 信息炸弹指攻击者在很短时间内向受害者的 QQ 发送大量的垃圾信息,开启无数个消息窗口,让 QQ 应接不暇,从而无法正常使用。这种"炸弹"极大地占用有限的网络带宽,阻塞网络,会导致用户上网速度变慢甚至无法上网,当大量的系统资源被占用后,还有可能造成系统瘫痪。造成 QQ 消息"炸弹"的主要原因是 QQ 本身的网络协议以及软件的设计存在着漏洞。

2. QQ 安全防范措施

针对 QQ 漏洞和 QQ 被炸等问题,作为 QQ 提供商腾讯公司应该组织人员完善 QQ 本身的网络协议和软件的设计,为用户提高安全的 QQ 使用程序,并及时提供升级的 QQ 版本,方便用户免费下载。

而作为普通的 QQ 用户,可以通过对 QQ 采取安全设置来防范,具体操作过程如下。

第 1 步:设置本地消息口令。

(1) 右击 QQ 图标,选择"系统设置"命令菜单,如图 8-3 所示。

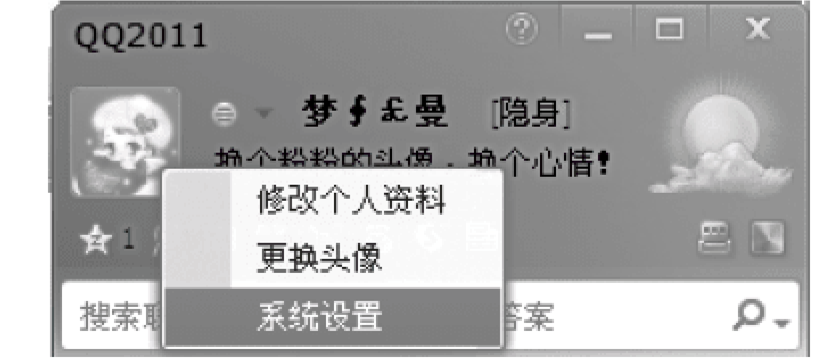


图 8-3　进入"系统设置"

(2) 在"系统设置"对话框的左侧框选择"安全设置"标签,在"安全设置"选项中选择"消息记录安全"选项,如图 8-4 所示。

(3) 在"消息记录加密"选项中勾选"启用消息记录加密"选项,同时在"启用消息记录加密"选项中的"口令"栏和"确认"栏中填入相应口令。

(4) 在"消息记录加密"选项中勾选"启用加密口令提示"选项,同时根据个人喜好在"启用加密口令提示"框中的"提示问题"栏和"问题答案"栏中输入问题和答案。

(5) 单击【确定】按钮完成设置。

此步设置可以防范 QQ 号被盗。

第 2 步:设置身份验证。

(1) 在图 8-4 中的"安全设置"框中选择"身份验证"选项。

(2) 进入"身份验证"对话框,如图 8-5 所示,根据个人需要,在身份验证框中勾选任一选项,此处以勾选"需要验证信息"选项为例。

(3) 单击【确定】按钮,完成设置。

此步设置可以防御如 QQ 通过自动查找和添加功能进行的信息炸弹攻击。



图 8-4 “系统设置”对话框



图 8-5 “身份验证”对话框

第 3 步：设置陌生人消息选项。

（1）在图 8-4 中的“安全设置”选项中选择“防骚扰设置”选项。

（2）在图 8-6 中的“防骚扰设置”对话框中的“陌生人消息”选项中勾选“不接收任何临时会话消息”选项。

（3）单击【确定】按钮即可。

此步设置可以防御 QQ 炸弹。



图 8-6 “防骚扰设置”对话框

此外用户还可以通过及时进行 QQ 漏洞的修补,安装防火墙加强系统的安全防护能力,使用代理登录 QQ 等措施来保护 QQ 安全。

8.2.4 网上购物的安全

1. 网上购物安全

网上购物就是把传统的商店直接“搬”进家,通过网络在家里直接购买自己需要的商品或者享受自己需要的服务。专业地讲,网上购物是电子商务具体应用的体现:一个或多个商家通过网站推销自己的产品,而消费者既可以是个人,也可以是企业。交易双方从洽谈、签约以及货款的支付、交货通知等整个交易过程通过网络一并完成,是电子商务的一个重要组成部分。

网上购物是通过网络完成购买,其特性决定了商品的虚拟性,购买者只能通过卖家对商品特征的描述来了解商品,充其量只能看到商品的实物图,并不能亲身体验商品的使用感觉,正确辨别商品质量。这就给了欺骗者可乘之机。一些卖家对于假冒伪劣商品的描述,使用专业网站的精美图片对商品进行夸大宣传,更有甚者通过文字游戏欺骗消费者,以次充好,以小充大,给网络市场造成了极大的破坏作用。同时他们以低价出售,有可能将好产品挤出网络市场,摧毁了消费者对网络购物的信任。

2. 网上购物安全保障措施

作为提供网上购物平台的网站应该从以下几个方面进行防范:

(1) 保证网站安全的网上购物系统首先必须具有一个安全、可靠的通信网络,以保证交易信息安全、迅速地传递;其次必须保证数据库服务器绝对安全,防止黑客闯入网络盗

取信息。因此首先要开发针对加密软件的技术,其次要开发出保证系统正常运行的技术。目前较广泛使用的网络安全技术有网络控制技术、密钥管理及加密算法技术、数字水印技术、防火墙技术等。而如此大规模的购物交易网站应采用多种保密技术综合、交叉地运行,同时更需要加强认证体系的建设,运用静态和动态的密码技术管理系统和数据库。

(2) 保证网站商家的质量。

作为大型的购物网站,应保证商家的质量,防止卖家出现网上购物的欺诈行为。首先,选择一些可靠的商家,其次,对自己网站的商家建立完善商家信任评价体系,对商家从商品质量、服务态度、物流速度等方面进行打分,对不符合要求的商家采取淘汰制度,为购买者提供一个安全可靠的购物环境。

此外,对于购物者来说,对网店的信用认证也是很重要的。在网络购物时应尽可能选择大型、知名度高的网站。对制作比较粗糙的网站和较为陌生的网站应采取一定的防范措施。在决定网上购物消费前,应通过电话、网络对经营者情况进行了解,如工商登记、信誉情况、经营规模及送货方式等,只有在确认主体合格、信誉度好时,才进行网络购物,并且应尽量选择货到付款和支付宝方式付款。

8.2.5 网上银行与网上支付的安全

1. 网上银行的概念

网上银行又称为网络银行、在线银行,是指银行利用 Internet 技术,通过 Internet 向客户提供理财开户、销户、查询、对账、行内转账、跨行转账、信贷、网上证券、投资理财等传统服务项目,使客户可以足不出户就能够安全便捷地管理活期和定期存款、支票、信用卡及个人投资等。可以说,网上银行是在 Internet 上的虚拟银行柜台。

网上银行又被称为"3A 银行",因为它不受时间、空间的限制,能够在任何时间(anytime)、任何地点(anywhere)、以任何方式(anyhow)为客户提供金融服务。

2. 网上支付的概念

网上支付是使消费者可以跨越时间和地域的限制,通过 Internet 来完成包括款项支付、资金调拨的电子转账及信息通知等多项业务,并具有实时支付效力的支付方式。对于网上支付,当前的主流方式是通过银行卡(包括信用卡、借记卡和支付卡等)这种支付工具,通过浏览器输入必要的支付认证信息,经发卡行认证授权后扣款完成在线支付。

3. 安全性分析

目前人们进行网上支付时一般使用网上银行进行支付。在这一过程中,网上银行作为网上支付提供者,其存在的安全问题主要有:

(1) 互联网安全风险。

由于互联网是采用开放式协议的公共网络,使得客户密码、客户隐私等敏感信息在传输过程中容易被截获、破译、篡改。而网上交易可以由客户随时随地发起交易请求,这一方面加大了银行识别客户身份、控制和规范客户行为的难度,另一方面,也使攻击者具有

隐蔽性，难以追踪相关责任人。同时，网上交易缺乏“白纸黑字”的凭证，电子交易凭证（如电子签名）又尚无法律效力，因此难以防范交易后的抵赖行为。此外，交易服务器是网上的公开站点，因而黑客入侵在所难免。

（2）后台支付系统安全性低。

网上银行系统使用了大量新技术、新产品，而这些新技术、新产品本身就可能存在安全漏洞和安全缺陷。同时，电子商务领域过度频繁的人才流动，增加了系统源码控制和设计机密性控制的难度，成为银行的安全隐患。而且，随着网上交易的频率越来越频繁，交易金额越来越大，更容易使其得到黑客的攻击，使后台支付系统安全性更难以保证。

对于网上支付的过程来说，其存在的风险主要有：

（1）支付密码泄露。

支付密码泄露是指带有键盘操作记录功能的木马进入系统后，录下所有用户输入的密码口令，然后将它们发送给木马制作者，于是黑客冒充持卡人通过互联网进行消费，给持卡人带来损失。

（2）支付数据被篡改。

支付数据被篡改是指攻击者修改互联网传输中的支付数据，达到谋利的目的，例如攻击者修改付款银行卡号、修改支付金额、修改收款人账号等。

4. 网上银行服务商可以采用的安全措施

针对上述的安全性分析，网上银行主要可以从以下几个方面进行防范：

（1）采用高安全级的 Web 应用服务器。

服务器使用可信的专用操作系统。凭借其独特的体系结构和安全检查，保证只有合法用户的交易请求能通过特定的代理程序送至应用服务器进行后续处理。

（2）设立防火墙，隔离相关网络。

网上银行中心系统可采用两道防火墙方案，保证网上银行中心系统和银行内部通信网的安全，实现网络分隔的要求。一道防火墙放在与互联网相连接的路由器（过滤路由器）后面，防止互联网用户的非法入侵，保护访问服务器的安全（防火墙软件可根据需要设置并根据安全监控系统提供的线索随时加以修改）；另一道防火墙用于网上银行中心系统与银行内部通信网的分隔，防止银行内部人员进入网银中心系统作案，同时防火墙的虚拟地址映射功能还可以对外隐藏实际的主机地址，达到减少攻击的目的。具体过程如图 8-7 所示。

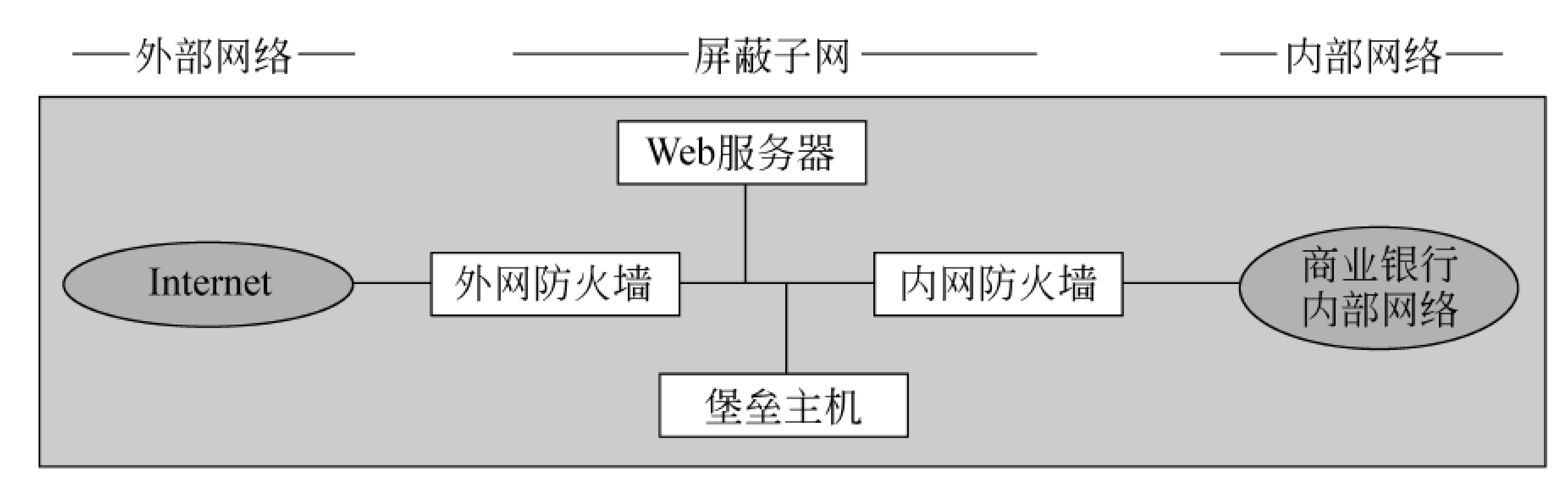


图 8-7　防火墙技术在网上银行中的应用

（3）实行身份识别和 CA 认证。

在网上银行系统中，用户的身份认证依靠基于“RSA 公钥密码体制”的加密机制、数字签名机制和用户登录密码的多重保证。银行对用户的数字签名和登录密码进行检验，全部通过后才能确认该用户的身份。用户的唯一身份标识就是银行签发的“数字证书”。用户的登录密码以密文的方式进行传输，确保了身份认证的安全可靠性。数字证书的引入，同时实现了用户对银行交易网站的身份认证，以保证访问的是真实的银行网站，另外还确保了客户提交的交易指令的不可否认性。由于数字证书的唯一性和重要性，各家银行为开展网上业务都成立了 CA 认证机构，专门负责签发和管理数字证书，并进行网上身份审核。

（4）建立安全的网络支付通道。

客户端登录到商业银行网上支付系统后，需要验证该系统的服务器数字证书可信性，以避免登录到假冒网站。客户端浏览器与商业银行支付系统间建立安全通道，该通道提供支付信息加密保障。客户端对支付信息数字签名，并发送到商业银行的支付系统。

（5）增强网络通信的安全性。

由于互联网是一个开放的网络，客户在网上传输的敏感信息（如密码、交易指令等）在通信过程中存在被截获、被破译、被篡改的可能。为了防止此种情况发生，网上银行系统一般都采用加密传输交易信息的措施，使用最广泛的是 SSL 数据加密协议。

SSL（secure socket layer，安全套接层）协议是一种安全通信协议，它能够对信用卡和个人信息提供较强的保护。SSL 是对计算机之间整个会话进行加密的协议。在 SSL 中，采用了公开密钥和私有密钥两种加密方法。在实际应用中，有两种支付方式采用该协议：账号直接传输方式和专用账号方式。账号直接传输方式是指客户在网上购物后把信用卡号直接传输给商家，传输过程中卡号信息用 SSL 协议加密。专用账号方式则是指商家在银行的协助下核实每一客户是否为银行卡持有人，并为每一个客户建立一个与银行卡对应的虚拟账号，每个虚拟账户都有独立的账号和密码。客户使用虚拟账户在互联网上付款时，账号和密码用 SSL 协议加密后传输到商家，这样可避免在网上直接使用银行卡的卡号和密码，保证了银行卡账户的安全。

（6）建立可信的网上支付后台系统。

金融业在 20 世纪 70 年代就已经开始将某些成本高的安全维护活动外包出去。外包也会让金融机构遭受风险。第三方可能按照自身想法开展某些活动或调整安全防御系统，而由于内部人员缺乏足够的技能，金融机构很难将已经外包的业务收回，即使能够收回，运营成本可能非常高。所以，除了要增强后台系统安全防御能力，防御互联网病毒、攻击威胁外，还应建立对第三方人员的授权管理和审计机制，严格约束外包人员的行为权限，任何涉及业务数据的操作都应取得主管部门授权，防止出现外包人员恶意篡改业务数据给用户和金融机构造成的损失。

此外，还可以采用 ISS 网络动态监控产品，实现 24 小时实时安全监控，进行系统漏洞扫描和实时入侵检测。

5. 网上银行客户可以采用的安全措施

作为网上银行的客户，要保证个人计算机的安全，增强安全意识。下面给出几点正确使用网上银行的几点建议：

(1) 核对网址。

客户开通网上银行要事先与银行签订协议。在登录网上银行时，必须核对登录的网址与协议书中的网址是否相符；登录网上银行网站时，尽量不要使用任何不可靠的链接方式，不要通过搜索引擎找到的网址或其他不明网站的链接途径进入，防止犯罪嫌疑人模仿银行网站盗取账户信息。

(2) 管好密码。

要避免设置与个人资料相关的简单密码。不要选用诸如身份证号码、出生日期、电话号码等作为支付密码；建议采用无规律的数字组合，提高支付密码被破解的难度；在不同的电子渠道上尽量使用不同密码；对不同的银行卡账户尽量设置不同的支付密码。

(3) 做好记录。

在进行网上银行交易时，要对录入信息(本人账号、金额等要素)进行仔细核对，做到"一慢、二看、三仔细、四清楚"，即"录入信息时要慢"、"按键时要准确查看"、"对录入的信息核对要仔细"、"对反馈回来的信息要记录清楚"。转账交易完成后不论系统提示成功与否，都要查询转出账户余额和明细。要定期查看历史交易明细并打印网上银行业务对账单，如发现异常交易或账务差错，应立即与银行联系，避免损失。

(4) 管好证书。

网上银行用户应避免在公共场合(如网吧、机场)和公用计算机上使用网上银行，防止数字证书等机密资料落入他人手中。最好不要安装 QQ 聊天程序、网络游戏等，尽量专机专用。

(5) 对异常动态提高警惕。

网上银行在系统运行稳定的情况下不会出现"系统维护"的提示。若遇重大事件，系统必须暂停服务，银行会提前公告客户。客户如不当心在陌生的"银行网址"上输入了银行卡号和密码，并遇到类似"系统维护"之类的提示。应立即拨打该银行客服热线进行确认，万一发现资料被盗，应立即修改相关交易密码或及时进行银行卡挂失。

此外，每次使用网上银行后，及时退出。如果个人资料有任何更改(例如，联系方式、地址等有变动)，请及时通过银行系统修改相关资料。

8.2.6 文件传输的安全

1. FTP 工作原理

FTP 是 TCP/IP 的一种具体应用，是网络中极为实用的服务之一。它是基于客户/服务器(C/S)模型而设计的，在客户端与 FTP 服务器之间建立两个连接。客户端用户调用 ftp 命令后，便与服务器建立连接，这一连接被称作控制连接，又称为协议解释器 PI，主要用于传输客户端的请求命令以及远程服务器的应答信息。一旦控制连接建立成功，双

方便进入交互式会话状态，互相协调完成文件传输工作。另一个连接是数据连接，当客户端用户向远程服务器提出一个 FTP 请求时，临时在客户与服务器之间建立一个数据连接，主要用于数据的传送，因而又称作数据传输过程 DTP。FTP 的协议模型如图 8-8 所示。

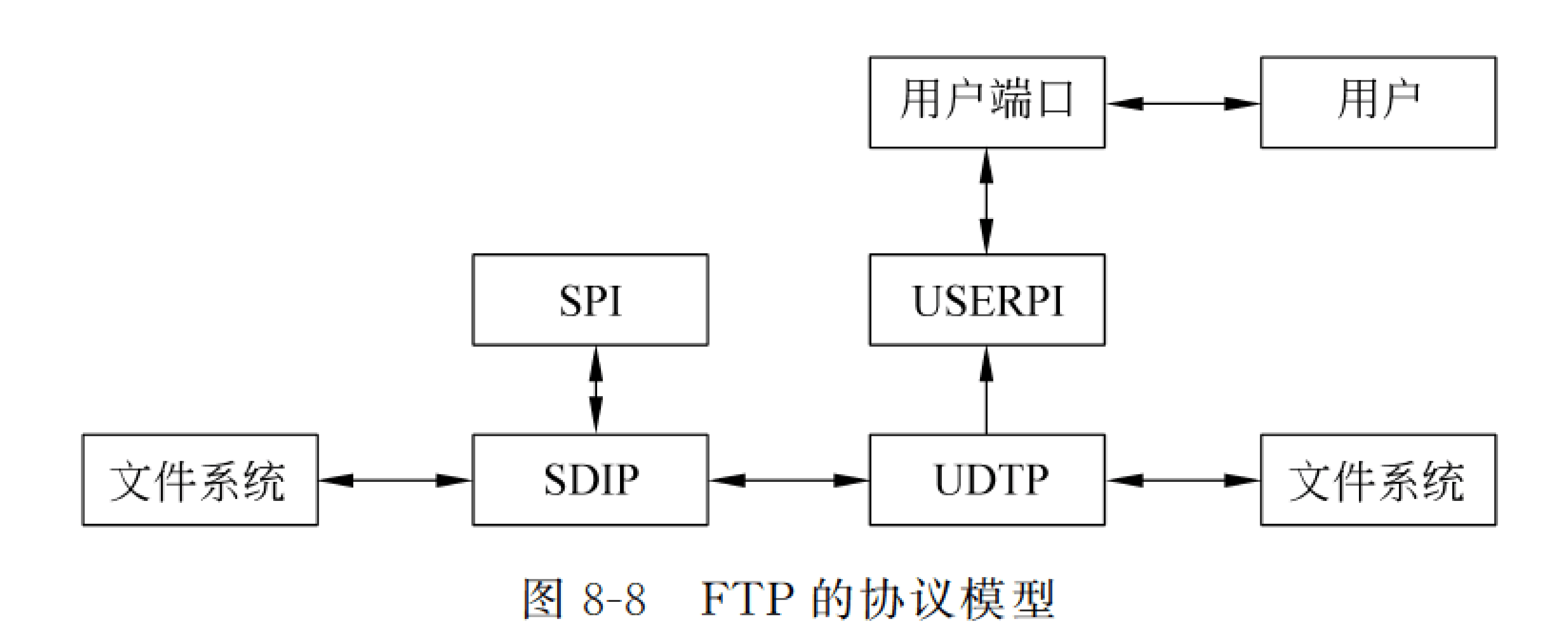


图 8-8　FTP 的协议模型

2. FTP 传输的安全策略

对于使用 FTP 传输的用户来说，FTP 传输的安全策略主要有限制端口和对服务器端软件进行安全设置。

端口是计算机和外部网络相连的逻辑接口，也是计算机的第一道屏障，端口配置正确与否直接影响到主机的安全，限制端口的方法比较多，可以使用第三方的个人防火墙，本书只介绍 Windows 自带的利用 TCP/IP 筛选功能进行防火墙设置的方法。此方法的操作过程如下：

第 1 步：打开“本地连接 属性”对话框。

(1) 打开“控制面板”对话框，找到“网络连接”图标。

(2) 在控制面板中右击“网络连接” 图标，选中“打开”命令菜单，如图 8-9 所示。



图 8-9　“控制面板”界面

(3) 右击“本地连接”，选中“属性”命令菜单，打开“本地连接 属性”对话框，如图 8-10 所示。

第 2 步：对端口进行设置。

(1) 在图 8-10“常规”标签下双击“Internet 协议(TCP/IP)”选项，进入“Internet 协议(TCP/IP) 属性”对话框，如图 8-11 所示。




图 8-10 “本地连接 属性”对话框

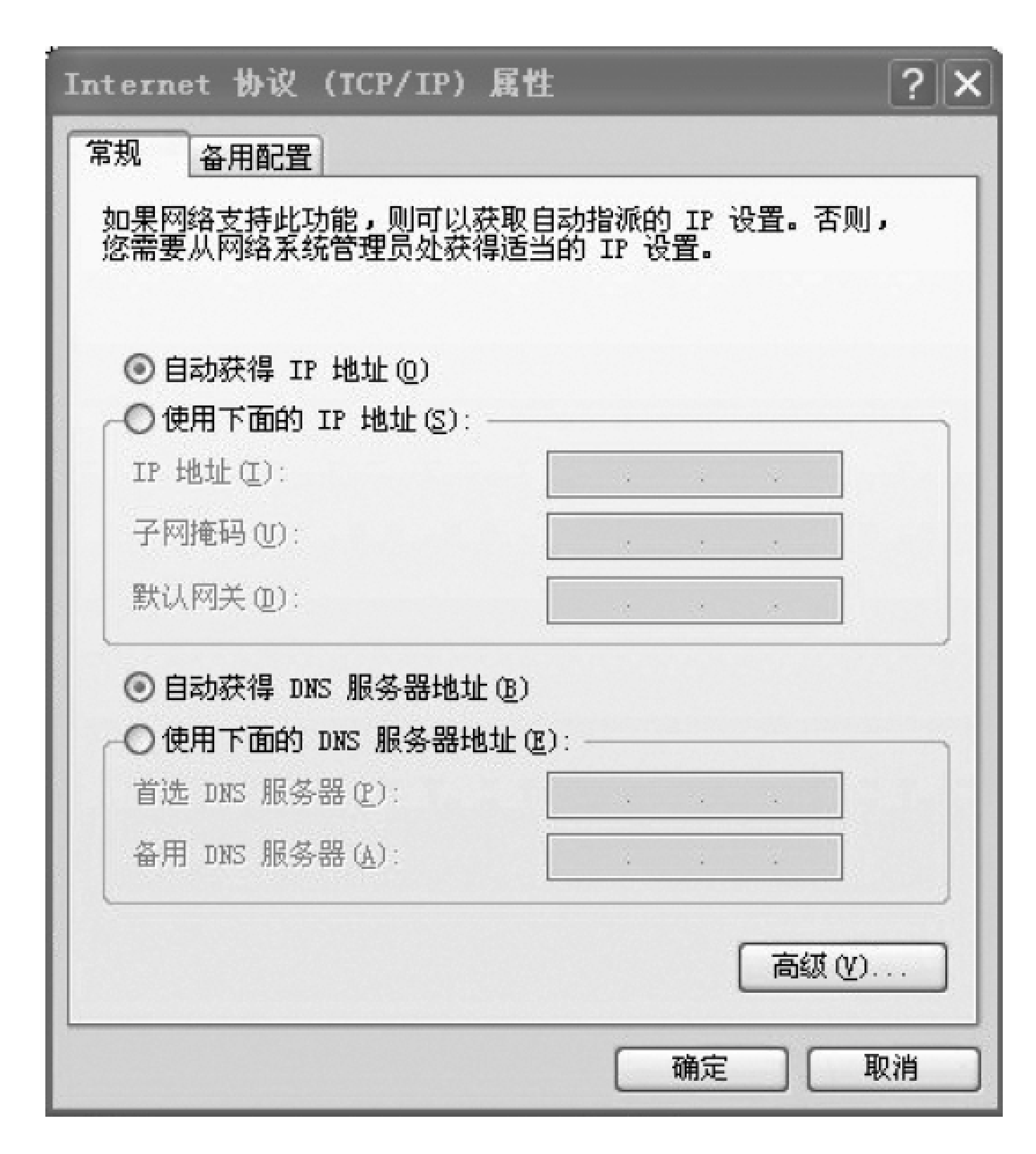


图 8-11 “Internet 协议（TCP/IP）属性”对话框

（2）在图 8-11 中单击【高级】按钮，打开“高级 TCP/IP 设置”对话框。如图 8-12 所示，在此对话框中选择“选项”标签。



图 8-12 “高级 TCP/IP 设置”对话框

（3）在图 8-12 中单击【属性】按钮，打开“TCP/IP 筛选”对话框，如图 8-13 所示。

（4）在图 8-13 中勾选“启动 TCP/IP 筛选”选项，并勾选“TCP 端口”框上方的“只允许”选项。

（5）在图 8-13 中单击【添加】按钮，在添加筛选框中输入允许的端口，本书以 21 号端口为例。

（6）在图 8-13 中单击【确定】按钮即完成设置。



图 8-13 “TCP/IP 筛选”对话框

3. 服务器端软件的安全设置

除了依靠系统提供的安全措施外,还需要利用 FTP 服务器端软件本身的设置来提高整个服务器的安全。对服务器端软件的安全设置可分为两种,一种是对 IIS 服务器端软件进行安全设置,另外一种是对 Serv-u(是一种被广泛运用的 FTP 服务器端软件)进行安全性设置。

(1) 对 IIS 服务器端软件进行安全设置。

一是及时安装新补丁;IIS 的安全性漏洞平均每两三个月就要出一两个漏洞。但微软会根据新发现的漏洞提供相应的补丁,这就需要不断更新,安装最新补丁。

二是将安装目录设置到非系统盘,关闭不需要的服务;一些恶意用户可以通过 IIS 的溢出漏洞获得对系统的访问权。把 IIS 安放在系统分区上,会使系统文件与 IIS 同样面临非法访问,容易使非法用户侵入系统分区。另外,由于 IIS 是一个综合性服务组件,每开设一个服务都将会降低整个服务的安全性,因而,对不需要的服务尽量不要安装或启动。

三是只允许匿名连接;FTP 最大的安全漏洞在于其默认传输密码的过程是明文传送,很容易被人嗅探到。而 IIS 又是基于 Windows 用户账户进行管理的,因而很容易泄露系统账户名及密码,如果该账户拥有一定管理权限,则更会影响到整个系统的安全。因此只允许匿名连接可以免却传输过程中泄密的危险。

四是谨慎设置主目录及其权限;IIS 可以将 FTP 站点主目录设为局域网中另一台计算机的共享目录,但在局域网中,共享目录很容易招致其他计算机感染的病毒攻击,严重时甚至会造成整个局域网瘫痪,因此,最好使用本地目录并将主目录设为 NTFS 格式的非系统分区中。这样,在对目录的权限设置时,可以对每个目录按不同组或用户来设置相应的权限。

五是尽量不要使用默认端口号 21;启用日志记录,以备出现异常情况时查询原因。

(2) 对 Serv-u 进行安全性设置。

与 IIS 的 FTP 服务相比,Serv-u 在安全性方面做得比较好,可以分别对“本地服务器”与域中的服务器进行安全方面的设置。

8.3　网络应用的安全技术

本节主要介绍网络应用中的安全技术，包括防钓鱼技术，防肉鸡技术，防监听技术和网络扫描技术等。

8.3.1　防钓鱼技术

网络钓鱼是指利用互联网进行的一种欺诈行为。它通过诱骗用户提供其个人账户和密码、信用卡信息、社保编号等个人资料，获得用户的某种身份信息，进而窃取用户的个人财产。

1. 网络钓鱼的主要方式

(1) 发送电子邮件，以虚假信息引诱用户中圈套。

以垃圾邮件的形式大量发送欺诈性邮件，这些邮件多以中奖、顾问、对账等内容引诱用户在邮件中填入银行账号和密码，或是以各种紧迫的理由要求收件人登录某网页提交用户名、密码、身份证号、信用卡号等信息，继而盗窃用户资金。

(2) 建立假冒网上银行、网上证券网站，骗取用户账号密码实施盗窃。

建立域名和网页内容都与真正网上银行系统、网上证券交易平台极为相似的网站，引诱用户输入账号密码等信息，进而通过真正的网上银行、网上证券系统或者伪造银行储蓄卡、证券交易卡盗窃资金；还有的利用跨站脚本，即利用合法网站服务器程序上的漏洞，在站点的某些网页中插入恶意 HTML 代码，屏蔽住一些可以用来辨别网站真假的重要信息，利用 cookies 窃取用户信息。例如曾出现过的某假冒银行网站，网址为 http://www.lcbc.com.cn，而真正的银行网站是 http://www.icbc.com.cn，犯罪分子利用数字 1 和字母 i 非常相近的特点企图蒙蔽粗心的用户。

(3) 利用虚假的电子商务进行诈骗。

建立电子商务网站，或是在比较知名、大型的电子商务网站上发布虚假的商品销售信息，犯罪分子在收到受害人的购物汇款后就销声匿迹。

(4) 利用木马和黑客技术等手段窃取用户信息后实施盗窃活动。

盗窃者通过发送邮件或在网站中隐藏木马等方式大肆传播木马程序，当感染木马的用户进行网上交易时，木马程序即以键盘记录的方式获取用户账号和密码，并发送给指定邮箱，用户资金将受到严重威胁。

(5) 利用用户弱口令等漏洞破解、猜测用户账号和密码。

不法分子利用部分用户贪图方便设置弱口令的漏洞，对银行卡密码进行破解。如 2004 年 10 月，3 名犯罪分子从网上搜寻某银行储蓄卡卡号，然后登录该银行网上银行网站，尝试破解弱口令，并屡屡得手。

实际上，不法分子在实施网络诈骗的犯罪活动过程中，经常采取以上几种手法交织、配合进行，还有的通过手机短信、QQ 及 MSN 进行各种各样的“网络钓鱼”不法活动。

2. 网络钓鱼的防范技术

针对不同的钓鱼手段,应该采取不同的反钓鱼技术。反钓鱼技术总地来说经历了原始的人工黑名单阶段、较有效的钓鱼特征码识别阶段及新兴的云安全实时拦截阶段。

(1) 黑白名单技术。

黑白名单技术是利用静态数据库列表,将已经发现的钓鱼网站记录到一个黑名单数据库,将可信站点列到白名单,当访问某网站的时候进行黑白名单对比,据此来判断所访问的网站是否为钓鱼网站。黑白名单技术实现很简单,但黑白名单是静态的,及时更新比较困难,特别是黑名单,因为网络钓鱼网站存活的时间一般很短,如不能及时更新,就不能及时有效地发现并制止钓鱼网站。

(2) 邮件过滤技术。

邮件过滤技术是指在邮件服务器端安装一个邮件过滤器,把有钓鱼内容的网页列入黑名单数据库,当用户访问到与黑名单中匹配的网页时,向用户发出一个警告。但随着新的钓鱼网页的不断出现,这种反钓鱼的技术就显得力不从心。

(3) 邮件认证技术。

电子邮件认证主要是通过加密及签名技术实现的。该技术有多种方式,可以对发件人 ID 进行认证,可以通过第三方可信机构对合法邮件域进行数字签名,还可以用对标题和消息本身进行加密认证。但是对邮件进行加密或签名会增加邮件服务器的负荷及 DNS 服务器的流量,并且该技术的实施,需要多方企业的合作。

(4) 特征识别技术。

特征识别技术突破了基于黑白名单这种静态的识别方法,是一种可测量的、可适时调整的服务。通过对钓鱼网页及钓鱼行为的分析,总结出钓鱼攻击的一些共同特征,然后对所要访问网页的对应特征进行评分,最后计算出其欺骗总分,看其是否超过给定的阀值,来判别其是否为钓鱼主页。主要对网站域名、URL、域指向、网页图片相似度、弹出对话框以及 SSL 协议的使用等方面进行分析。

(5) 蜜罐及蜜网技术。

蜜罐技术是指故意设置一些特征引诱攻击者攻击,继而对系统中所有的操作和行为进行监控和记录,然后通过研究和分析这些记录,得到攻击者采用的攻击工具、手段,攻击目的和攻击水平等信息,进而采取相应的反攻击措施。蜜网技术是在蜜罐技术基础上发展来的,是一种高交互型的用来获取广泛的安全威胁信息的蜜罐,是由多个蜜罐以及防火墙、入侵防御系统、系统行为记录、自动报警、辅助分析等一系列系统和工具所组成的一整套体系结构,这种体系结构创建了一个高度可控的网络,使得安全研究人员可以控制和监视其中的所有攻击活动。因此,一旦钓鱼者对蜜网进行攻击,安全分析人员就能及时在蜜网捕获的监控和日志数据的基础上,对网络钓鱼攻击的整个生命周期有一个完整的理解,并能深入剖析钓鱼者所使用的技术手段和工具,提供潜在的漏洞威胁预警。

(6) “云安全”技术。

“云安全”就是一个巨大的互联网安全系统,是网络时代信息安全的最新体现,它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念,通过网状的大量客户端监

测网络中软件行为的异常，获取互联网中木马、恶意程序的最新信息，并将检测的信息推送到服务器端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。只要用户成为云安全系统的客户端，就能够共享所有互联用户的安全信息。无论哪个网民中毒，访问挂马网页或是访问钓鱼网站，云安全系统都能够第一时间作出反应，及时采取相应的措施，避免其他用户再受欺骗。但是云安全技术的实施必须有海量的客户端，需要有专业的技术和经验，还需大量的资金投入和合作伙伴的加入，需要条件较高。

3. 个人对网络钓鱼的防范措施

(1) 针对电子邮件欺诈，如收到有如下特点的邮件就要提高警惕，不要轻易打开和听信：一是伪造发件人信息，如 123@adebank.com；二是问候语或开场白往往模仿被假冒单位的口吻和语气，如“亲爱的用户”；三是索取个人信息，要求用户提供密码、账号等信息；四是邮件内容多为传递紧迫的信息，例如声称若不及时进行某项操作，就会造成某些可怕的后果，如关闭服务或者是取消账户等。还有一类邮件是以超低价或免税等为诱饵诱骗消费者。

(2) 针对假冒网上银行、网上证券网站的情况，在进行网上交易时要注意做到以下几点：一是核对网址，看是否与真正网址一致；二是选取和保管好密码，不要选诸如身份证号码、出生日期、电话号码等作为密码，建议用字母、数字混合密码，尽量避免在不同系统使用同一密码；三是做好交易记录，对网上银行、网上证券等平台办理的转账或支付等业务做好记录，定期查看“历史交易明细”和打印业务对账单，如发现异常交易或差错，立即与有关单位联系；四是管理好数字证书，避免在公用的计算机上使用网上交易系统；五是对异常动态提高警惕，如不小心在陌生的网址上输入了账户和密码，并遇到类似“系统维护”之类提示时，应立即拨打有关客服热线进行确认，万一资料被盗，应立即修改相关交易密码或进行银行卡、证券交易卡挂失；六是通过正确的程序登录支付网关，通过正式公布的网站进入，不要通过搜索引擎找到的网址或其他不明网站的链接进入。

(3) 针对虚假电子商务信息的情况，应掌握以下诈骗信息特点，不要上当：一是虚假购物、拍卖网站看上去都比较“常规”，有公司名称、地址、联系电话、联系人、电子邮箱等，有的还留有互联网信息服务备案编号和信用资质等；二是交易方式单一，消费者只能通过银行汇款的方式购买，且收款人为个人，而非公司，订货方法一律采用先付款后发货的方式；三是诈取消费者款项的手法如出一辙，当消费者汇出第一笔款后，骗子会来电以各种理由要求汇款人再汇余款、风险金、押金或税款之类的费用，否则不会发货，也不退款，一些消费者由于第一笔款已汇出，抱着侥幸心理继续再汇；四是在进行网络交易前，要对交易网站和交易对方的资质进行全面的了解。

此外，还有其他网络安全措施：一是安装防火墙，防病毒软件，并经常升级；二是注意经常给系统打补丁，堵塞软件漏洞；三是禁止浏览器运行 JavaScript 和 ActiveX 代码；四是不要上一些不太了解的网站，不要执行从网上下载后未经杀毒处理的软件，不要打开 MSN 或者 QQ 上传送过来的不明文件等；五是提高自我保护意识，注意妥善保管自己的私人信息，如本人证件号码、账号、密码等，不向他人透露；尽量避免在网吧等公共场所使用网上电子商务服务。

8.3.2 防肉鸡技术

“肉鸡”是指被黑客攻破，种植了木马病毒的计算机，黑客可以随意操纵它并利用它做任何事情。“肉鸡”可以是各种系统，如 Windows XP 或 Linux，也可以是一家公司、企业、学校甚至政府军队的服务器。

1. 成为“肉鸡”的可能性分析

检测个人计算机是否成为肉鸡可以从以下方面进行分析：

(1) QQ、MSN 的异常登录提醒（系统提示上一次的登录 IP 不符）。

(2) 网络游戏登录时发现装备丢失或与上次下线时的位置不符，甚至用正确的密码无法登录。

(3) 鼠标突然不听使唤，在不动鼠标的时候，鼠标也会移动，并且还会单击有关按钮进行操作。

(4) 正常上网时，突然感觉很慢，硬盘灯在闪烁。

(5) 在没有使用网络资源时，发现网卡灯在不停闪烁。如果设定为连接后显示状态，还会发现屏幕右下角的网卡图标在闪。

(6) 服务列队中出现可疑的程序服务。

(7) 防火墙失去对一些端口的控制。

(8) 上网过程中计算机重启。

(9) 有些程序如杀毒软件、防火墙卸载时出现闪屏（卸载界面一闪而过，然后报告完成）。

(10) 一些用户信任并经常使用的程序（QQ 杀毒）卸载后。目录文件仍然存在，删除后自动生成。

(11) 计算机运行过程中或者开机的时候弹出莫名其妙的对话框。

(12) 通过 CMD 下输入 NETSTAT -AN 查看是否有可疑端口等。

(13) 注意检查防火墙软件的工作状态。例如 360 防火墙。若在网络状态页，显示当前正在活动的网络连接，仔细查看相关连接。如果发现自己根本没有使用的软件在连接到远程计算机，就要小心了。

2. 防止个人计算机成为肉鸡的安全技术

通常按默认方式安装的操作系统，如果不做任何安全加固，那么其安全性难以保证。攻击者稍加利用便可使其成为肉鸡。因此，防止个人计算机成为肉鸡的方式主要有两种，一是利用操作系统自身功能加固系统，二是使用安全软件加固操作系统。本书所有内容都基于 Windows XP 系统。

利用操作系统自身功能加固系统的方法主要有：

(1) 加强系统登录账户和密码的安全。

系统设置的密码应当符合复杂性和最小长度的要求，不仅要包括常用英文字母、数字、字母大小写，最好还可以加入特殊字符（如@等），而且密码的字符数不应该小于 8 位。

另外，为了防止黑客通过默认账户登录系统，应该为管理员账号设置密码并禁用 guest 账户。

（2）取消远程协助和远程桌面连接。

右击桌面“我的电脑”图标，选择“属性”命令菜单，在“系统属性”对话框中选择“远程”标签，取消“远程协助”和“远程桌面连接”复选框选项。

（3）禁用危险的系统服务。

在 Windows XP 系统中，一些端口与相应的系统服务是相关联的，有的服务还与系统中的特定端口相关联，例如 Terminal Services 服务与 3389 端口关联。因此，禁用一些不需要的服务，不仅能降低系统资源消耗，而且能增强系统安全性。

单击桌面“开始”→“运行”菜单命令，在“运行框”中输入 services. msc，按 Enter 键后进入“服务”对话框。在此对话框中禁用以下服务：

```
NetMeeting Remote Desktop Sharing
Remote Desktop Help Session Manager
Remote Registry
Routing and Remote Access
Server
TCP/IP NetBIOS Helper
Telnet
Terminal Services
```

（4）关闭 137、138、139 端口。

右击桌面“网上邻居”图标，选择“属性”命令菜单，在“本地连接”对话框中打开“Internet 协议（TCP/IP）”的属性对话框。在此对话框中，单击【高级】按钮，选择“WINS”标签，在“NetBIOS 设置”框中勾选“禁用 TCP/IP 上的 NetBIOS”选项，关闭 137、138 和 139 端口。

（5）启动系统审核策略。

在桌面单击“开始”→“运行”菜单命令，在“运行”框中输入 gpedit. msc，打开“组策略”对话框，选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在“策略”框中启用“审核登录事件”、“审核对象访问”、“审核系统事件”和“审核账户登录事件”为“成功”方式的审核。

（6）用户权利指派。

在组策略对话框中，通过“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”，最后在用户权利指派框中，将“从网络访问此计算机”策略中的所有用户都删除，在“拒绝从网络访问此计算机”策略中确保已有“everyone”账户，然后再删除“通过终端服务允许登录”策略中的所有用户，并确保在“通过终端服务拒绝登录”策略中有“everyone”账户。

（7）禁用系统默认共享。

在“组策略”对话框中，通过选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”选项，在“策略”框中将“网络访问：不允许 SAM 账户的匿名枚

举”及“网络访问：不允许 SAM 账户和共享的匿名枚举”全部启用；将“网络访问：可匿名访问的共享”、“可匿名访问的管道”及“可远程访问”注册表中的全部内容删除。最后，打开“资源管理器”，选择“工具”下拉菜单中的“文件夹选项”命令菜单，在出现的“文件夹选项”对话框中单击“查看”标签，然后在“高级设置”框中，取消“使用简单文件共享”选项。

对加固操作系统安全性而言，还可以通过安装相应的安全软件来进一步增强系统的安全性能。主要的安全软件有杀毒软件、防火墙、代理服务器。杀毒软件主要用来防止黑客通过木马来控制主机；安装第三方防火墙来限制系统中能够与互联网通信的进程和应用程序；通过使用 HTTP 代理和在计算机上安装简单的代理软件可以隐藏公网 IP 地址，将增加黑客的攻击行为的难度。

8.3.3　防监听技术

1. 网络监听概念

网络监听又称为网络嗅探，这是一种在他方未察觉的情况下捕获其通信报文或通信内容的技术。在网络安全领域，网络监听技术对于网络攻击与防范都有着重要意义。它被广泛应用于网络维护和管理，是网络管理员深入了解网络当前的运行状况、测试网络数据流量、实时监控网络的有力助手。对黑客而言，网络监听是一种有效的信息收集手段，并且可以辅助进行 IP 欺骗，其只接收不发送的特性也使其拥有良好的隐蔽性。

网络监听技术的能力范围目前仅限于局域网，在目前以以太网为主的局域网环境下，网络监听技术具有原理简单、易于实现、难以被察觉的优势。

2. 网络监听技术

目前，以太网已经成为局域网组网技术的绝对主流。在以太网的通信环境中主要有两种网络连接方式：共享式网络和交换式网络。

(1) 共享网络下的网络监听技术。

在共享传输介质的以太网中，网络中的任何一个节点都会接收到在信道中传输的数据帧。接下来节点将如何处理该数据帧，取决于数据帧的真实目的地址和节点网卡的接收模式。

处于监听模式下的主机可以嗅探到同一个网段下的其他主机发送信息的数据包。网卡接收到数据包后，就会将其传给上一层来处理，如果在这一阶段使用监听软件来提供一定的捕获和过滤机制，就可以达到监听人们所希望知道的信息的目的。

(2) 交换式网络下的监听技术。

交换式以太网是用交换机或其他非广播式交换设备组建成的局域网。这些设备收到的数据帧中的 MAC 地址决定数据帧应发向交换机的哪个端口。由于端口间的传输彼此屏蔽，在很大程度上解决了网络监听的困扰，但随着监听技术的发展，交换以太网中也存在网络监听的安全隐患。其主要的安全隐患有溢出攻击和 ARP 欺骗。

3. 网络监听的防御

（1）使用安全的网络拓扑结构。

安全的网络拓扑结构通常称为网络分段，其目的是将非法用户与敏感的网络资源相互隔离。将网络划分为不同的网段，各段之间无法进行直接的通信。只有相互信任的主机才在同一网段，进行直接通信，网段外的主机无法直接对网段内的主机进行监听。通过网络分段将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

（2）数据通道加密。

目前这种技术主要有两种方式，一种是建立各种数据传输加密通道，另一种是对数据内容进行加密。

数据通道加密是指建立各种数据传输加密通道，正常的数据都是通过事先建立的通道进行传输的，如果对通道进行加密，则许多应用协议中明文传输的账号、口令等敏感信息将受到严密的保护。目前的数据通道加密方式主要有 SSH、SSL 和 VPN。SSH 是一种介于传输层与应用层之间的加密通道协议，提供了一种安全的身份认证级数据加密机制，还可以对传输的数据进行压缩，能够有效地防止网络监听、IP 欺骗、DNS 欺骗等攻击行为。

SSL 是在浏览器和 Web 服务器之间建立一条安全的数据传输通道，利用公钥机制还可以做到浏览器与服务器之间的相互认证。目前，大多数商业 Web 服务器和浏览器都支持 SSL 协议，而且，SSL 也不仅仅可以应用在 Web 服务的安全访问上，事实上，许多传统的网络应用都可以用 SSL 作为其安全支撑。

VPN 主要是利用公共网络组建私人的专用网络从而达到安全传输数据的目的。目前 VPN 在 OSI 参考模型的不同层次上都可以实现，在安全数据传输中得到了广泛的应用。

（3）数据内容加密。

数据内容加密是对数据内容进行加密，它利用目前较为可靠的加密机制来对互联网上传输的文件和数据进行加密。其中较为完善的有邮件加密机制 PGP 和网络认证协议 Kerberos。邮件加密机制 PGP 是通过数字签名和内容加密，保证了邮件传输中的机密性和可认证性。PGP 主要是用作邮件传输的加密解密，也可以对文件进行加解密，此外，还可以对邮件或文件进行数字签名，保证其可认证性。网络认证协议 Kerberos 则提供了一种在开放式网络环境下进行身份认证的方法，它使网络上的用户可以相互证明自己的身份，其采用对称密钥体制对信息进行加密。

（4）利用 ARP 数据包进行监测。

使用 ARP 数据包进行监测是指向局域网内的主机发送非广播方式的数据包，包中的 IP 地址是网络中不存在的地址，如果局域网内的某个主机响应了这个 ARP 请求以自己的 MAC 地址作为回应，那么就可以判断它很可能就是处于网络监听模式了。除此之外也可以建立 MAC 数据库，把网内所有网卡的 MAC 地址记录下来，每个 MAC 和 IP 地理位置统统装入数据库，以便及时查询备案。这是目前相对而言比较好的监测模式。

（5）观测被检测主机的响应时间。

主机的响应时间是指目标主机对测试数据包的平均响应时间。观测被检测主机的响应时间的过程是测试主机首先利用 ICMP 请求及响应，计算出目标计算机的平均响应时间。在得到这个数据后，测试主机再次向本地网络发送大量的伪造数据包。与此同时再次发送测试数据包以确定目标主机的平均响应时间的变化值，通过平均响应时间的变化值来判断目标主机是否是监听主机。

8.3.4 网络扫描技术

网络扫描技术是一种基于 Internet 远程监测目标网络或本地主机安全性脆弱点的技术，是一种主动防御技术。其基本原理是采用模拟黑客攻击的方式对目标可能存在的已知安全漏洞进行逐项检测，以便对工作站、服务器、交换机、数据库等各种对象进行安全漏洞检测。借助于扫描技术，人们可以发现网络和主机存在的对外开放的端口、提供的服务、某些系统信息、错误的配置、已知的安全漏洞等。故安全扫描技术是一种极为有效的主动防御技术，能发现隐患于未然，如果结合入侵检测系统和防火墙等其他安全技术，能为网络提供全方位的保护。

网络扫描技术是一柄双刃剑，系统管理员可以通过它保护网络安全；入侵者也可以利用它来攻击网络。

根据扫描对象不同，网络扫描技术可分为端口扫描、操作系统扫描与漏洞扫描。

1. 端口扫描

端口扫描是指向目标主机的 TCP/IP 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，从而可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入或流出 IP 数据包来监视本地主机的运行情况，它仅能对接收到的数据进行分析，帮助发现目标主机的某些内在的弱点。常见的端口扫描技术包括 TCP connect 扫描、TCP SYN 扫描以及秘密扫描。

（1）TCP connect 扫描。

TCP connect 扫描是 TCP 端口扫描的基础，也是最直接的端口扫描方法。它尝试与远程主机的端口建立一次正常的 TCP 连接，若连接成功则表示目标端口开放。它实现起来非常容易，使用系统提供的 connect()函数来连接目标端口，尝试与目标主机的某个端口建立一次完整的三次握手过程，如果目标端口正处于监听状态，connect()就成功返回，否则返回－1，表示端口不可访问。

这种扫描方法的优点是实现简单，对操作者的权限没有严格要求，另一优点是扫描速度快，但缺点是会在目标主机的日志记录中留下痕迹，易被发现，并且数据包会被过滤掉。

（2）TCP SYN 扫描。

TCP SYN 扫描是指扫描程序向目标主机发送 SYN 数据段，如果收到的应答是 SYN/ACK，那么说明目标端口处于监听状态。如果收到的应答是 RST，说明目标端口是关闭的。扫描程序在收到应答之后不管是何种应答，都向目标主机发送一个 RST/ACK 分组。这样，虽然没有建立一个完整的 TCP 连接，但扫描程序也能从目标主机的应答中

知道目标主机的某个端口是否开放。

TCP SYN 扫描的优点是比 TCP connect 扫描更隐蔽,服务器端可能不会留下日志记录。其缺点是在大部分操作系统下,扫描主机需要构造适用于这种扫描的 IP 包,而通常情况下,构造自己的 SYN 数据包必须要有 root 权限。

(3) 秘密扫描。

秘密扫描是一种不被审计工具检测的扫描技术,它能躲避 IDS、防火墙、包过滤器和日志审计,获取目标端口开放或关闭的信息。由于没有包含 TCP 三次握手协议的任何部分,所以无法被记录下来,比半连接扫描更为隐蔽。但这种扫描的缺点是扫描结果的不可靠性会增加,而且扫描主机也需要自己构造 IP 包。

2. 操作系统扫描

(1) 应用层扫描技术。

通过向目标主机发送应用服务连接或访问目标主机开放的有关记录就可能扫描出目标主机的操作系统(包括相应的版本号)。

(2) TCP/IP 堆栈特征扫描技术。

TCP/IP 堆栈特征扫描技术有:

① FIN 扫描:通过发送一个 FIN 数据包到一个打开的端口,并等待回应。RFC793 定义的标准行为是“不”响应,但诸如 Windows,BSD,CISCO 等操作系统会回应一个 RESET 包。大多数的扫描器都使用了这项技术。

② BOGUS 标记位扫描:通过发送一个 SYN 包,它含有没有定义 TCP 标记的 TCP 头。那么在 Linux 系统的回应中仍旧会包含这个没有定义的标记,而在一些别的系统则会在收到该包之后关闭连接。利用这个特性,可以区分一些操作系统。

③ TCP ISN 取样:这是利用寻找初始化序列规定长度与特定的操作系统相匹配的方法。利用它可以对许多系统分类,如较早的 UNIX 系统是 64K 长度。一些新的 UNIX 系统则是随机增长的长度,而 Windows 平台则使用“基于时间”方式产生的 ISN 会随着时间的变化而有着相对固定的增长。

3. 漏洞扫描

漏洞扫描就是通过采用一定的技术主动地去发现系统中的安全漏洞。漏洞扫描可以分为对未知漏洞的扫描和对已知漏洞的扫描。未知漏洞扫描的目的在于发现软件系统中可能存在但尚未发现的漏洞。已知漏洞的扫描主要是通过采用模拟黑客攻击的方式对目标可能存在的已知安全漏洞进行逐项扫描,可以对工作站、服务器、交换机、数据库等各种对象进行安全漏洞扫描,检测是否存在已公布的安全漏洞。漏洞扫描技术是建立在端口扫描技术和远程操作系统识别技术的基础之上的,漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞:

(1) 特征匹配方法。

基于网络系统漏洞库的漏洞扫描的关键部分就是它所使用的漏洞特征库。通过采用基于规则的模式特征匹配技术,即根据安全专家对网络系统安全漏洞、黑客攻击案例的分

析和系统管理员对网络系统安全配置的实际经验，可以形成一套标准的网络系统漏洞库，然后在此基础之上构成相应的匹配规则，由扫描程序自动进行漏洞扫描。若没有被匹配的规则，系统的网络连接是禁止的。

（2）插件技术。

插件是由脚本语言编写的子程序，扫描程序可以通过调用它来执行漏洞扫描，检测出系统中存在的一个或多个漏洞。添加新的插件就可以使漏洞扫描软件增加新的功能，扫描出更多的漏洞。

4. 扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的软件工具。它集成了常用的各种扫描技术，能自动发送数据包去探测和攻击远端或本地的端口和服务，能自动收集和记录目标主机的反馈信息，从而发现目标主机是否存活、目标网络内所使用的设备类型与软件版本、服务器或主机上各 TCP/UDP 端口的分配、所开发的服务、所存在的可能被利用的安全漏洞，还可以提供一份可靠的安全性分析报告，报告远程或本地主机可能存在的脆弱性。扫描器操作简便，效率高，极大节省了人力资源。

在 Internet 安全领域，扫描器已成为最常用的安全工具之一。

5. 针对入侵者扫描的防范措施

（1）关闭闲置端口，禁止不必要服务。

扫描的目的是获得目标系统的信息，检查主机开放的端口情况和可能存在的漏洞。系统上开放的端口，运行的服务都可能为入侵提供信息，成为入侵者攻击的目标。因此，对抗扫描最基本的措施是将系统上不必要的服务全部禁止，一个扫描不出太多信息的系统通常都会使得入侵者放弃对其攻击的企图。

（2）屏蔽敏感信息。

系统中很多看起来没什么用的信息往往对入侵者来说尤为重要，入侵者通过这些信息，能判断出操作系统的类型、服务的版本等，然后才能进行相应的攻击。当这些敏感信息被屏蔽之后，攻击者对目标主机也就无从下手了。

（3）合理配置网络安全设备。

这种预防端口扫描的方式显然用户自己是不可能手工完成的，或者说完成起来相当困难，需要借助软件，如常用的网络防火墙或入侵检测系统（IDS）。防火墙和入侵检测系统是目前最常用的安全产品，配置合理的网络安全设备能过滤大多数扫描，即使有扫描能穿过防火墙，这个扫描行为也会被防火墙的日志系统记录下来，而配置合理的 IDS 也同样能发现和记录大部分的扫描行为。

（4）陷阱技术。

可以使用目前较为流行的“蜜罐”（Honeypot）技术来设置一个陷阱，用路由器把攻击者引导到一个蜜罐上。即将一个不断受到扫描的系统更换 IP 和主机名，并在原来位置设置一个蜜罐或一个空系统，这种方式能帮助收集最新的扫描，并判断有什么样的扫描能穿过防火墙进入目标系统中。

8.4 应用实例

8.4.1 使用 Sniffer Pro 软件监测流量信息

Sniffer Pro 是一款便携式网管和应用故障诊断分析软件,不管是在有线网络还是在无线网络中,它都能够给予网络管理人员实时的网络监视、数据包捕获以及故障诊断分析能力。下面介绍如何在个人计算机使用此软件。

1. 安装网络监测软件 Sniffer Pro

第 1 步:到网上下载 Sniffer Pro 软件程序包。

第 2 步:解压 Sniffer Pro 程序包,进入起始安装界面,如图 8-14 所示。



图 8-14 起始安装界面

第 3 步:完成安装。

(1) 按安装向导进行几步操作后进入最终安装界面,如图 8-15 所示。



图 8-15 最终安装界面

(2) 单击【完成】按钮,软件安装成功。

2. 查询流量信息

第 1 步:启动 Sniffer 程序。

通过:“开始”→“所有程序”→“Sniffer Pro”→“Sniffer”来运行该程序。

第 2 步:选择监听网卡。

(1) 在图 8-16 中单击“File”菜单,选择其下拉框中的“Select Settings”菜单命令,如图 8-16 所示。

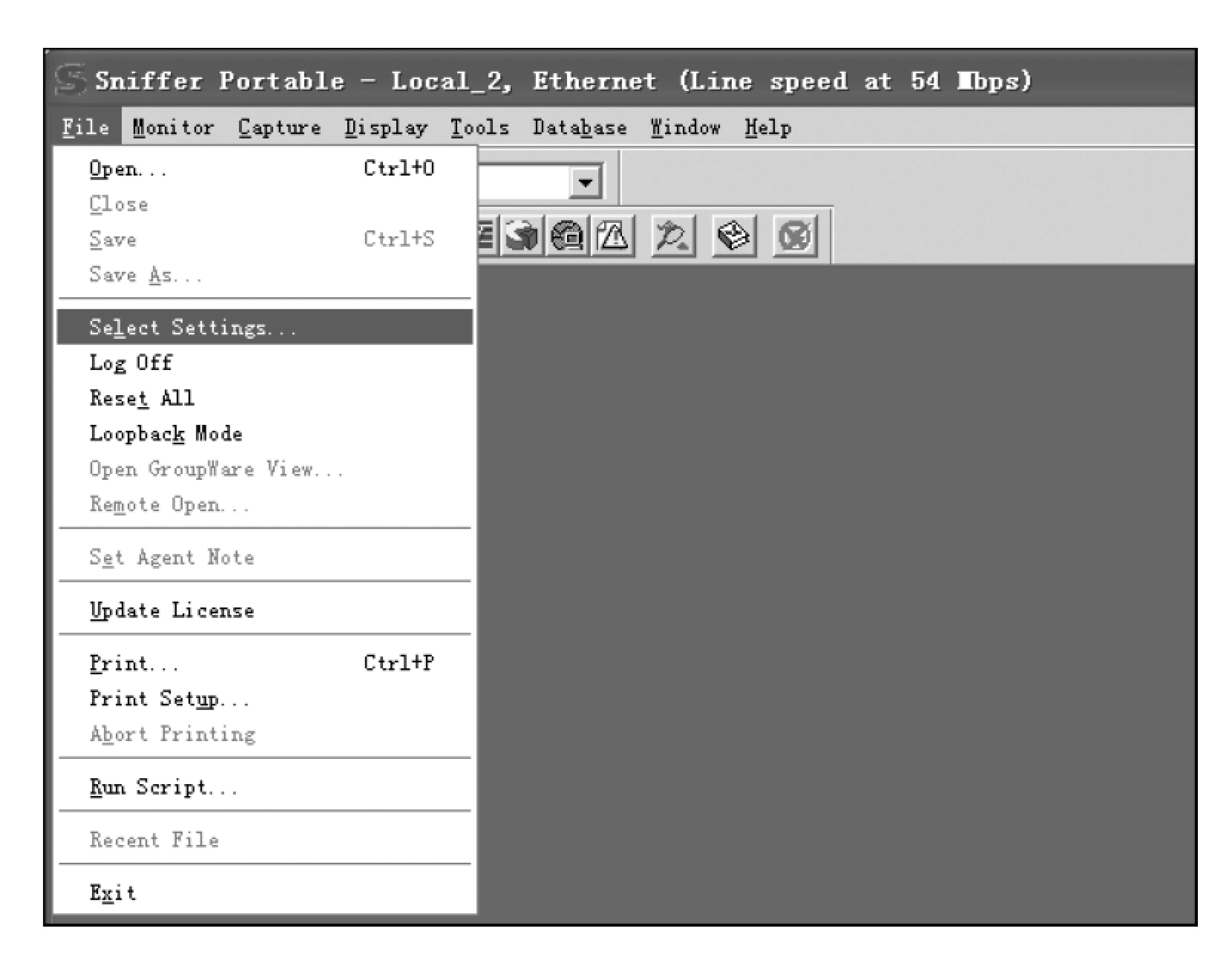


图 8-16 进入网卡选择窗口

(2) 在图 8-17 中选择想监听的网卡,单击【确定】按钮,即完成选择。

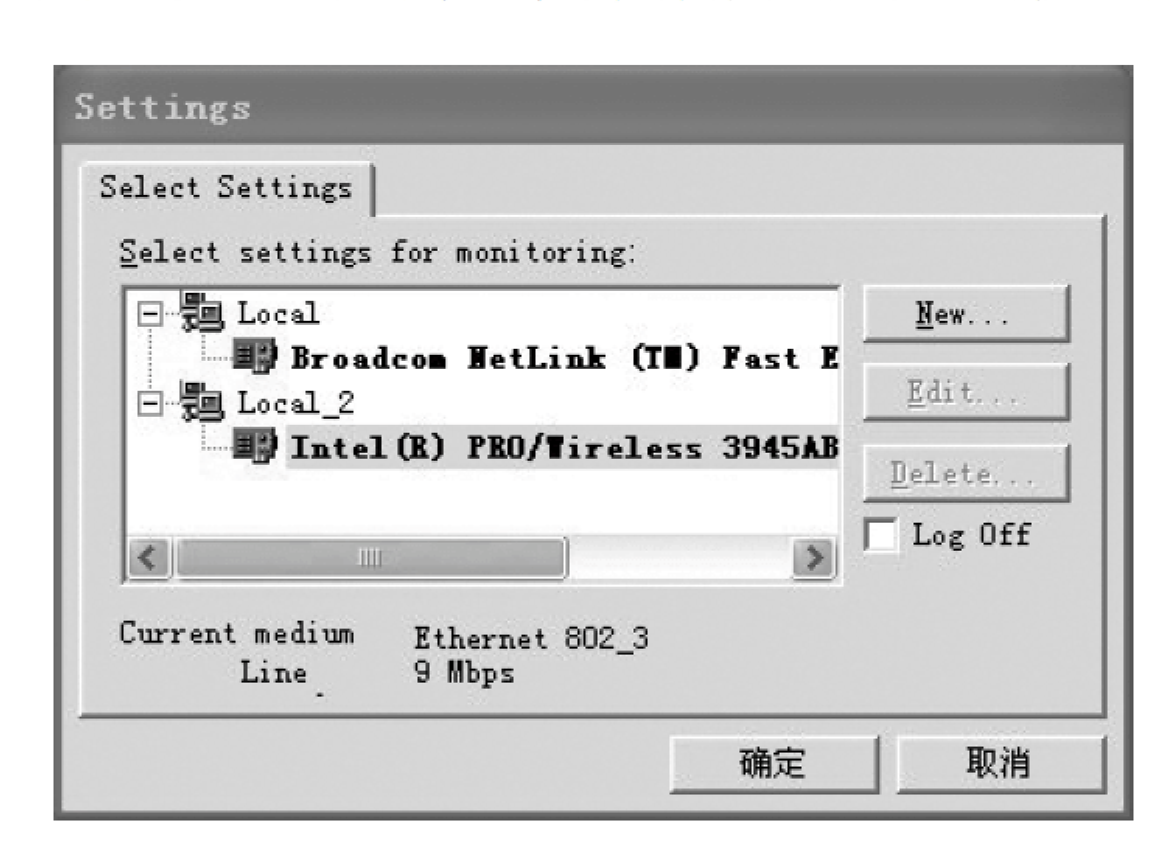


图 8-17 选择监听网卡对话框

第 3 步:监视网卡流量。

(1) 单击图 8-16 中的图标按钮,进入网卡监视窗口,如图 8-18 所示。

(2) 在图 8-18 中,最左边的类似汽车仪表的图像称为“Utilization%网络使用率”,此

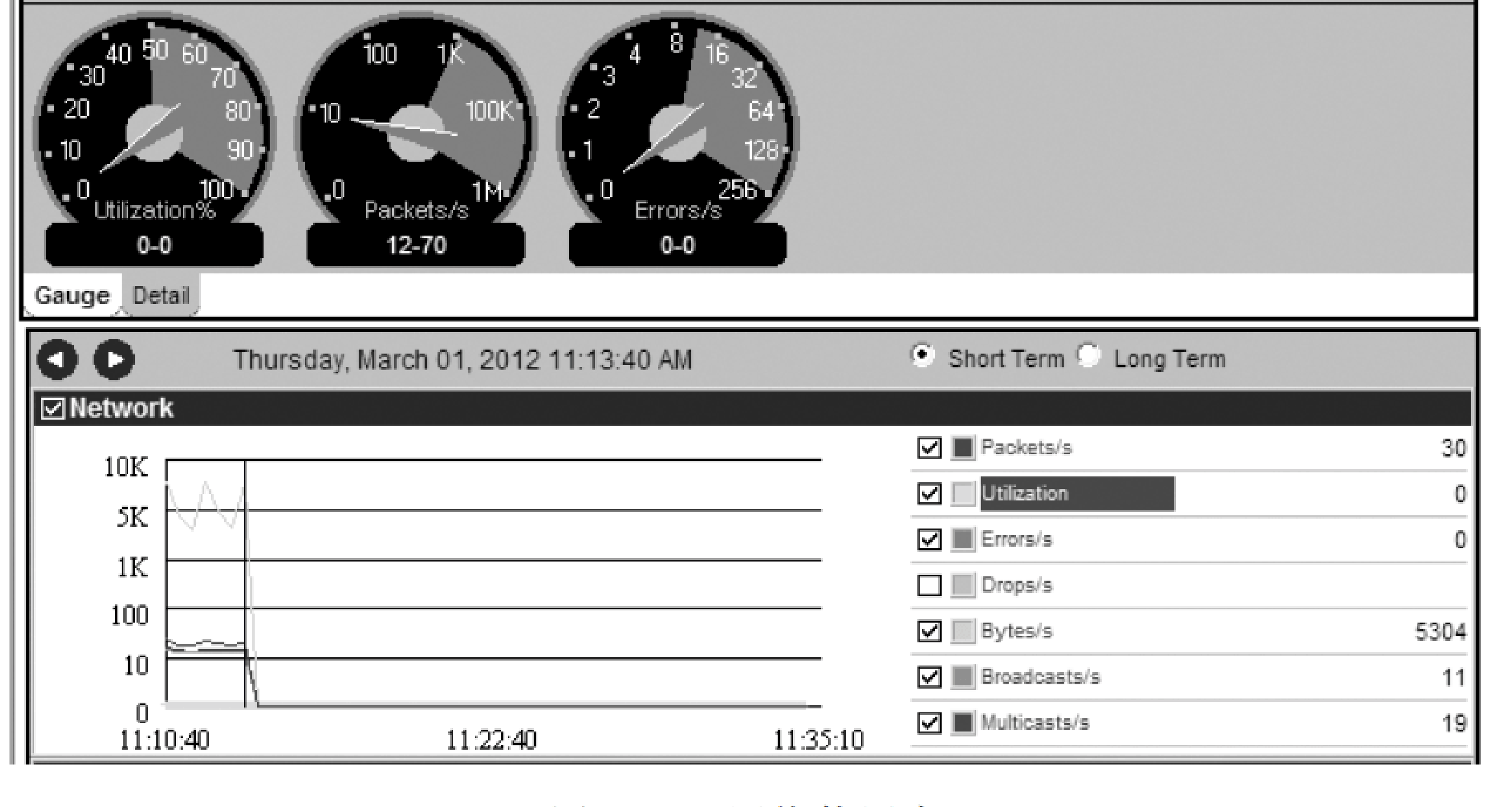


图 8-18　网络使用率

图像中的指针指向 0，表示此时网络使用率为 0，同时，勾选仪表下方“Network 框”中的右边选项“Utilization”，则会在 Network 的绘制图中会出现一条较粗的绿色线，此线也表示网络使用率，其对应的横轴坐标值为网络使用率大小。

(3) 图 8-19 中间的类似汽车仪表的图像称为“Packets/s 数据包传输率”，图 8-19 中“Packets/s”图像中的指针偏向 10 上方位置，同时，仪表下方显示的范围是 17～126，代表数据包传输率在 17～126 之间变化。此外，勾选仪表下方“Network 框”中的右边选项“Packets/s”，则会在 Network 下方的绘制图中出现一条较粗的蓝色线，此线表示数据包传输率大小，其对应的横轴坐标值为数据包传输率大小，为 21packets/s。

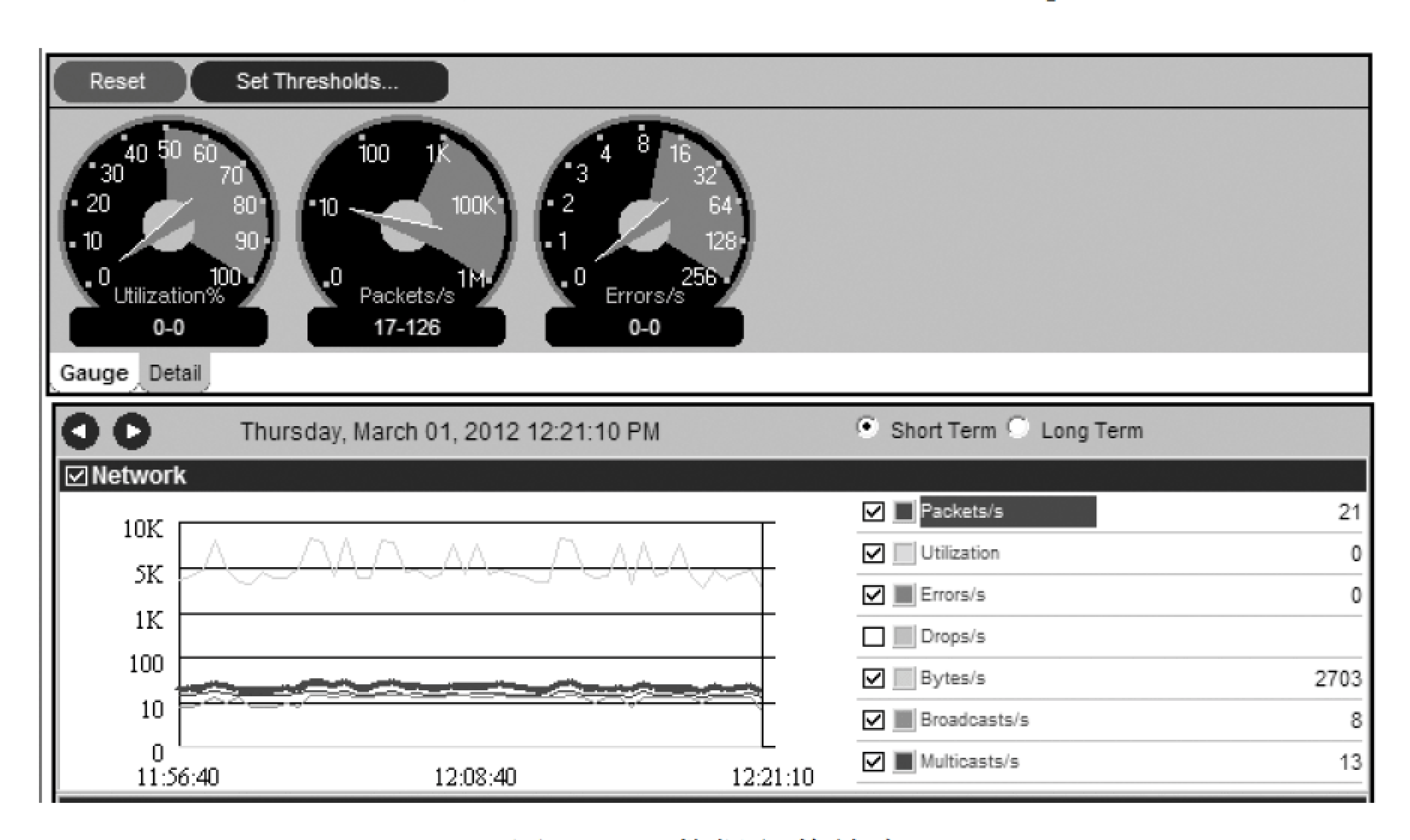


图 8-19　数据包传输率

(4) 图 8-19 中最右边的类似汽车仪表的图像称为“Errors/s 错误数据情况”，图 8-18 中“Errors/s”图像处的指针指向 0，表示此时错误数据情况为 0；勾选仪表下方“Network 框”中的右边选项“Errors/s”，则会在 Network 下方的绘制图中出现一条较粗的红色线，

其对应的横轴坐标值为错误数，如图 8-20 所示。

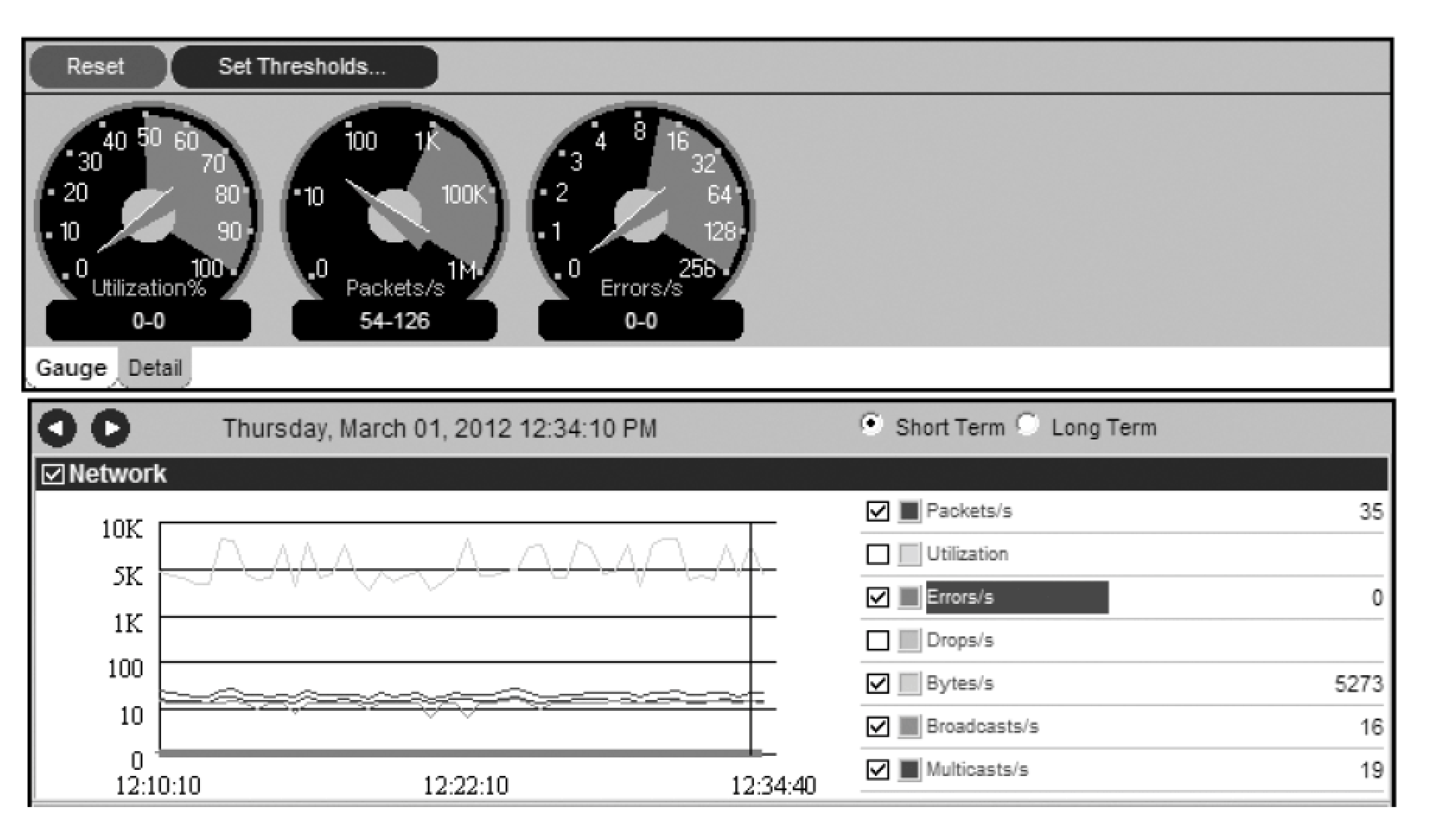


图 8-20　错误数据情况

若在图 8-18 中有指针指向红色区域就说明网络线路不好或者网络使用压力负荷太大。一般浏览网页的情况和图 8-18 显示的类似，网络使用率不高，传输情况也是 9～30 个 Packets/s，错误数基本没有。

第 4 步：统计各项具体数据。

（1）单击图 8-18 中仪表下方的“Detail 标签”，会出现如图 8-21 所示的列表。

Reset　Set Thresholds...　Show Total　Show Average Rate(per second)

Network		Size Distribution		Detail Errors	
Packets	546	64 Bytes	46	CRCs	0
Drops	0	65-127 Bytes	191	Runts	0
Broadcasts	281	128-255 Bytes	130	Oversizes	0
Multicasts	265	256-511 Bytes	28	Fragments	0
Bytes	69,402	512-1023 Bytes	10	Jabbers	0
Utilization	0	1024-1518 Bytes	1	Alignments	0
Errors	0			Collisions	0

Gauge　Detail

No data　Short Term　Long Term

图 8-21　Detail 列表 1

（2）在图 8-21 的右上方位置选择“Show Total”选项，则会显示图 8-21 所示的 Detail 列表 1，Detail 列表 1 显示各项数据信息。

（3）在图 8-21 的右上方位置选择“Show Average Rate(per second)”选项，则会显示图 8-22 所示的 Detail 列表 2，Detail 列表 2 是各项数据的平均速率。

第 5 步：设置参数最大上限。

（1）单击图 8-18 中仪表上方的“set thresholds”标签，出现如图 8-23 所示的参数设置对话框。

（2）根据需要对所有参数的名称和最大显示上限进行设置，设置完成后单击【确定】按钮。

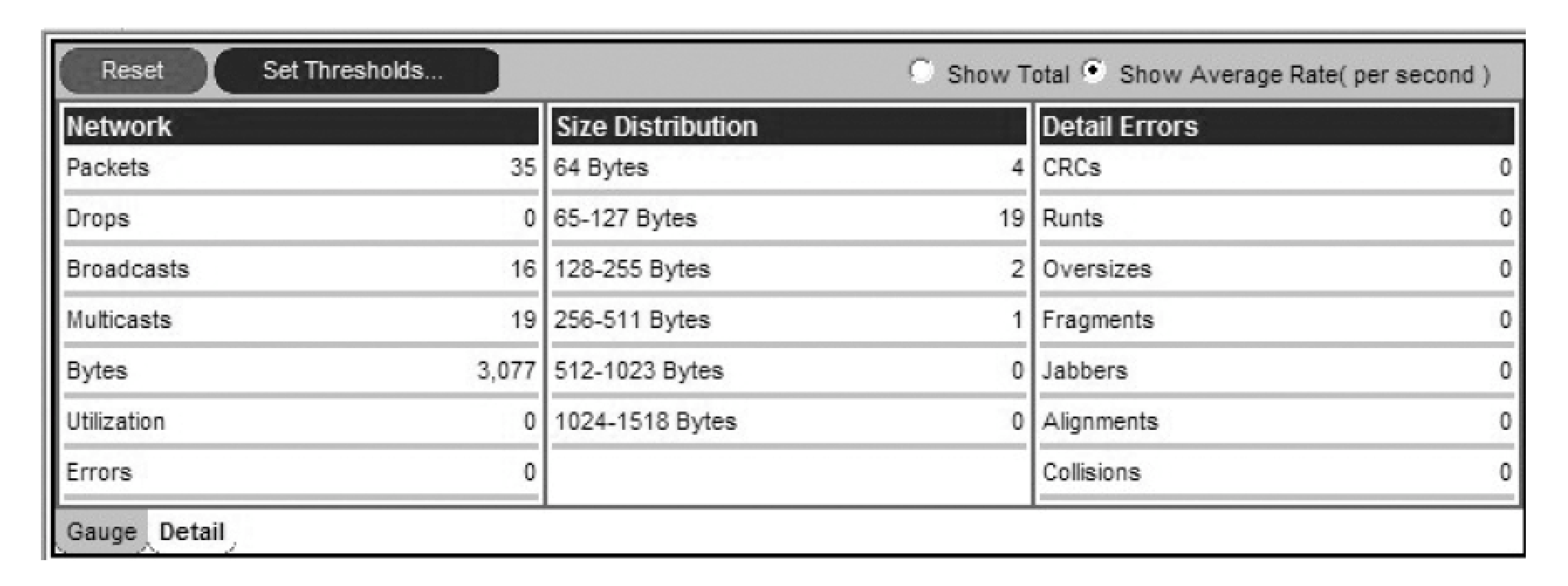


图 8-22　Detail 列表 2

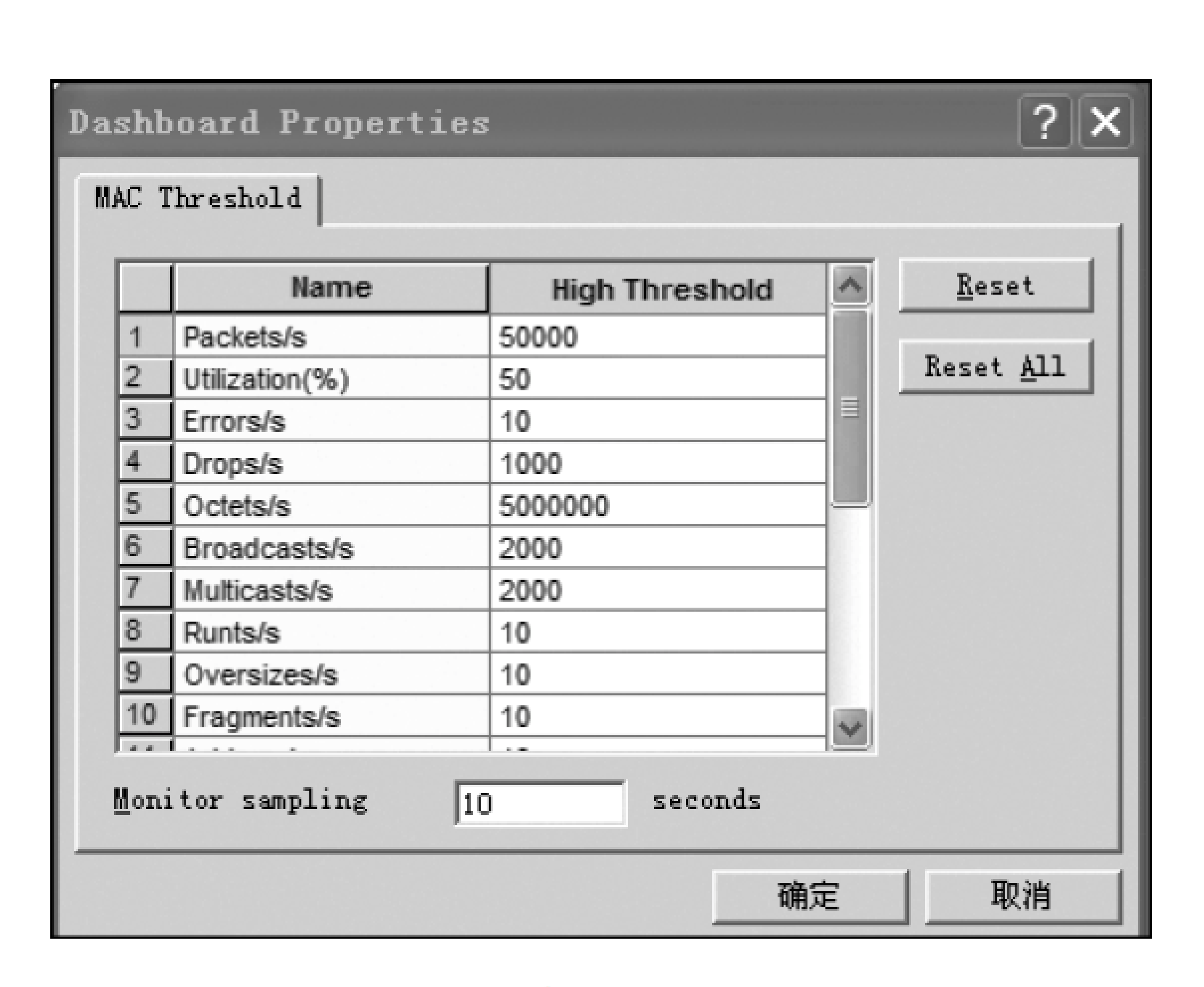


图 8-23　参数设置对话框

第 6 步：查看本机和网络其他地址的数据交换情况。

(1) 在图 8-24 中单击“Monitor”菜单，选择其下拉框中的“Host Table”，进入“Host Table”列表，如图 8-25 所示。

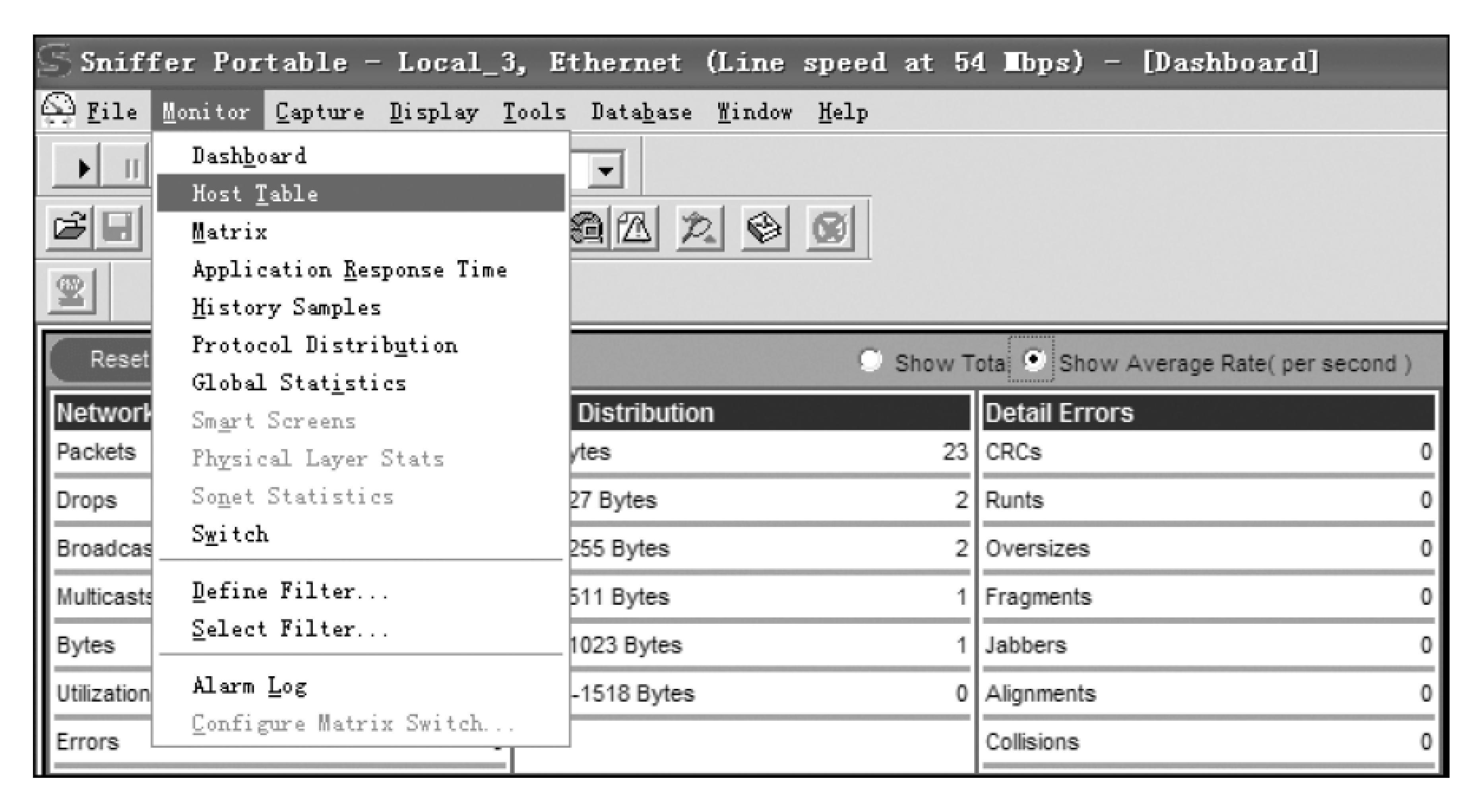
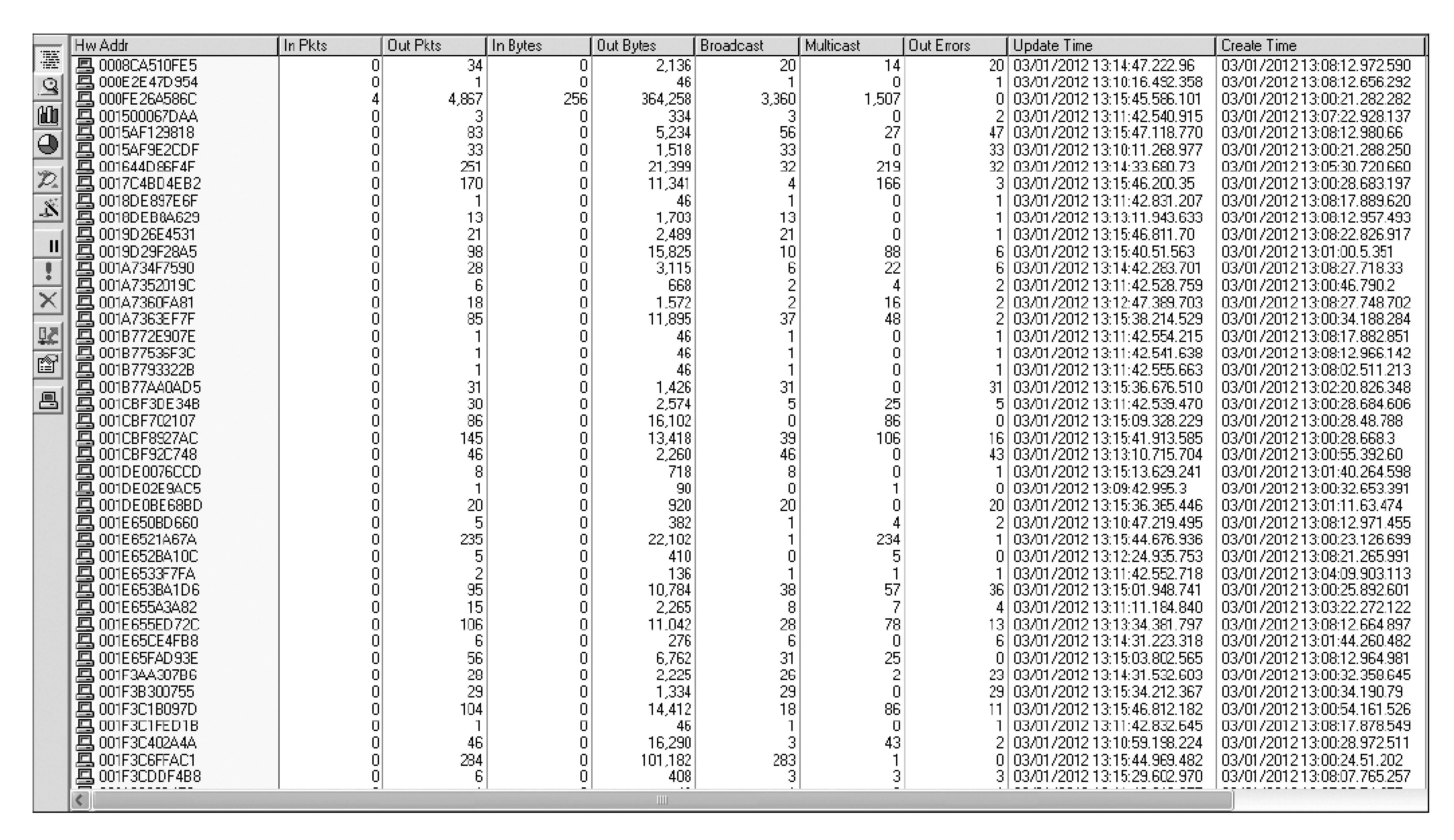


图 8-24　进入 Host Table

(2) 在图 8-25 中查看本机和网络中其他地址的数据交换情况表，此表中包括“输入



Hw Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broadcast	Multicast	Out Errors	Update Time	Create Time
0008CA510FE5	0	34	0	2,136	20	14	20	03/01/2012 13:14:47.222.96	03/01/2012 13:08:12.972.590
000E2E47D954	0	1	0	46	1	0	1	03/01/2012 13:10:16.492.358	03/01/2012 13:08:12.656.292
000FE26A586C	4	4,867	256	364,258	3,360	1,507	0	03/01/2012 13:15:45.586.101	03/01/2012 13:00:21.282.282
001500067DAA	0	3	0	334	3	0	2	03/01/2012 13:11:42.540.915	03/01/2012 13:07:22.928.137
0015AF129818	0	83	0	5,234	56	27	47	03/01/2012 13:15:47.118.770	03/01/2012 13:08:12.980.66
0015AF9E2CDF	0	33	0	1,518	33	0	33	03/01/2012 13:10:11.268.977	03/01/2012 13:00:21.288.250
001644D86F4F	0	251	0	21,399	32	219	32	03/01/2012 13:14:33.680.73	03/01/2012 13:05:30.720.660
0017C4BD4EB2	0	170	0	11,341	4	166	3	03/01/2012 13:15:46.200.35	03/01/2012 13:00:28.683.197
0018DE897E6F	0	1	0	46	1	0	1	03/01/2012 13:11:42.831.207	03/01/2012 13:08:17.889.620
0018DEB8A629	0	13	0	1,703	13	0	1	03/01/2012 13:13:11.943.633	03/01/2012 13:08:12.957.493
0019D26E4531	0	21	0	2,489	21	0	1	03/01/2012 13:15:46.811.70	03/01/2012 13:08:22.826.917
0019D29F28A5	0	98	0	15,825	10	88	6	03/01/2012 13:15:40.51.563	03/01/2012 13:01:00.5.351
001A734F7590	0	28	0	3,115	6	22	6	03/01/2012 13:14:42.283.701	03/01/2012 13:08:27.718.33
001A7352019C	0	6	0	668	2	4	2	03/01/2012 13:11:42.528.759	03/01/2012 13:00:46.790.2
001A7360FA81	0	18	0	1,572	2	16	2	03/01/2012 13:12:47.389.703	03/01/2012 13:08:27.748.702
001A7363EF7F	0	85	0	11,895	37	48	2	03/01/2012 13:15:38.214.529	03/01/2012 13:00:34.188.284
001B772E907E	0	1	0	46	1	0	1	03/01/2012 13:11:42.554.215	03/01/2012 13:08:17.882.851
001B77536F3C	0	1	0	46	1	0	1	03/01/2012 13:11:42.541.638	03/01/2012 13:08:12.966.142
001B7793322B	0	1	0	46	1	0	1	03/01/2012 13:11:42.555.663	03/01/2012 13:08:02.511.213
001B77AA0AD5	0	31	0	1,426	31	0	31	03/01/2012 13:15:36.676.510	03/01/2012 13:02:20.826.348
001CBF3DE34B	0	30	0	2,574	5	25	5	03/01/2012 13:11:42.539.470	03/01/2012 13:00:28.684.606
001CBF702107	0	86	0	16,102	0	86	0	03/01/2012 13:15:09.328.229	03/01/2012 13:00:28.48.788
001CBF8927AC	0	145	0	13,418	39	106	16	03/01/2012 13:15:41.913.585	03/01/2012 13:00:28.668.3
001CBF92C748	0	46	0	2,260	46	0	43	03/01/2012 13:13:10.715.704	03/01/2012 13:00:55.392.60
001DE0076CCD	0	8	0	718	8	0	1	03/01/2012 13:15:13.629.241	03/01/2012 13:01:40.264.598
001DE02E9AC5	0	1	0	90	0	1	0	03/01/2012 13:09:42.995.3	03/01/2012 13:00:32.653.391
001DE0BE68BD	0	20	0	920	20	0	20	03/01/2012 13:15:36.365.446	03/01/2012 13:01:11.63.474
001E650BD660	0	5	0	382	1	4	2	03/01/2012 13:10:47.219.495	03/01/2012 13:08:12.971.455
001E6521A67A	0	235	0	22,102	1	234	1	03/01/2012 13:15:44.676.936	03/01/2012 13:00:23.126.699
001E652BA10C	0	5	0	410	0	5	0	03/01/2012 13:12:24.935.753	03/01/2012 13:08:21.265.991
001E6533F7FA	0	2	0	136	1	1	1	03/01/2012 13:11:42.552.718	03/01/2012 13:04:09.903.113
001E653BA1D6	0	95	0	10,784	38	57	36	03/01/2012 13:15:01.948.741	03/01/2012 13:00:25.892.601
001E655A3A82	0	15	0	2,265	8	7	4	03/01/2012 13:11:11.184.840	03/01/2012 13:03:22.272.122
001E655ED72C	0	106	0	11,042	28	78	13	03/01/2012 13:13:34.381.797	03/01/2012 13:08:12.664.897
001E65CE4FB8	0	6	0	276	6	0	6	03/01/2012 13:14:31.223.318	03/01/2012 13:01:44.260.482
001E65FAD93E	0	56	0	6,762	31	25	0	03/01/2012 13:15:03.802.565	03/01/2012 13:08:12.964.981
001F3AA307B6	0	28	0	2,225	26	2	23	03/01/2012 13:14:31.532.603	03/01/2012 13:00:32.358.645
001F3B300755	0	29	0	1,334	29	0	29	03/01/2012 13:15:34.212.367	03/01/2012 13:00:34.190.79
001F3C1B097D	0	104	0	14,412	18	86	11	03/01/2012 13:15:46.812.182	03/01/2012 13:00:54.161.526
001F3C1FED1B	0	1	0	46	1	0	1	03/01/2012 13:11:42.832.645	03/01/2012 13:08:17.878.549
001F3C402A4A	0	46	0	16,290	3	43	2	03/01/2012 13:10:59.198.224	03/01/2012 13:00:28.972.511
001F3C6FFAC1	0	284	0	101,182	283	1	0	03/01/2012 13:15:44.969.482	03/01/2012 13:00:24.51.202
001F3CDDF4B8	0	6	0	408	3	3	3	03/01/2012 13:15:29.602.970	03/01/2012 13:08:07.765.257

图 8-25　本机和网络中其他地址的数据交换情况表

数据包 InPkts"、"流出数据包 OutPkts"以及其他交换数据等。

（3）在图 8-26 中单击"Monitor"菜单，选择其下拉框中的"Matrix"，进入 Matrix 界面。

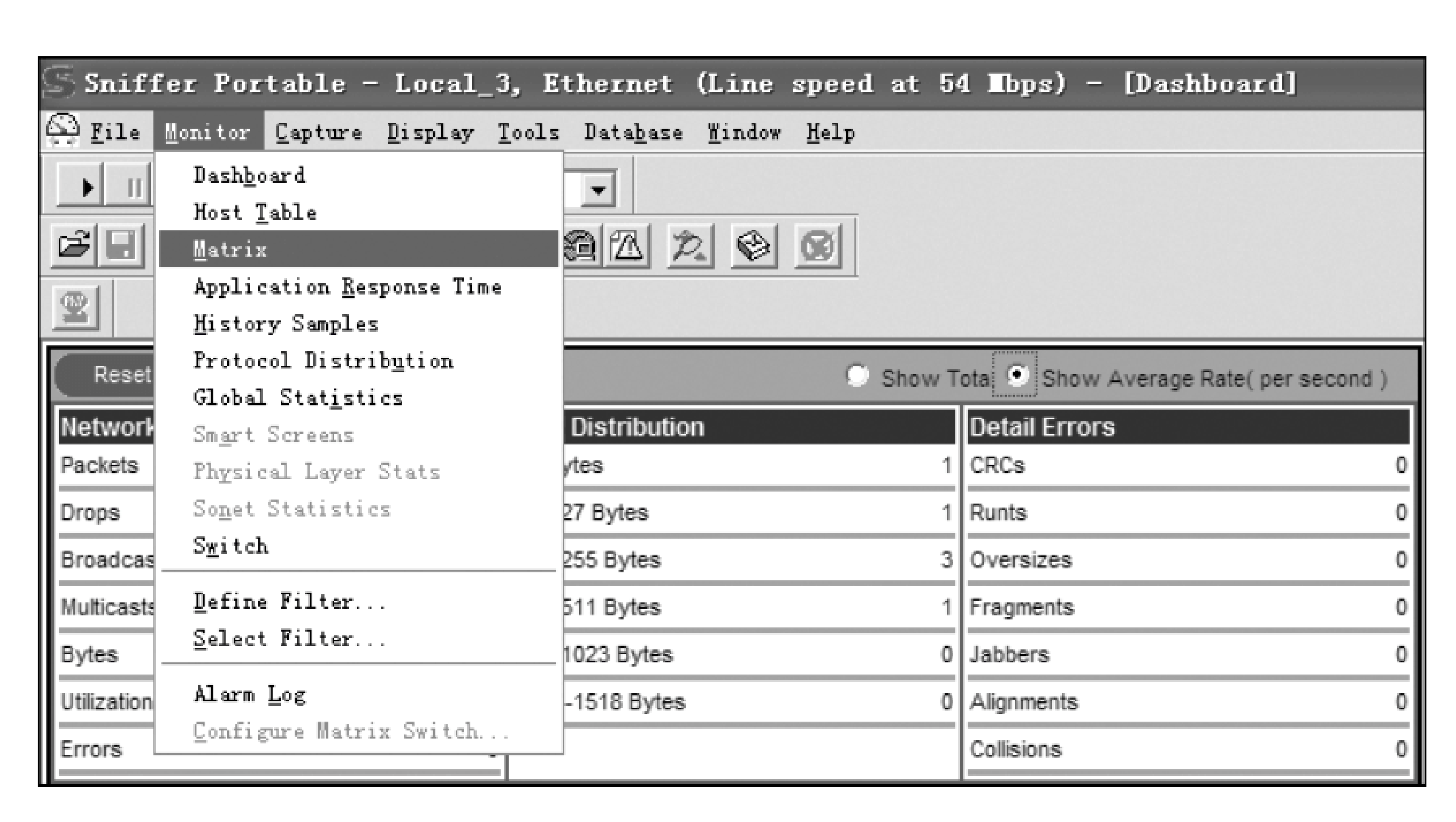


图 8-26　进入 Matrix 界面

（4）在图 8-27 中观察本机与网络其他地址的流量图，图中连线的粗细决定了数据流量的多少。

8.4.2　端口扫描工具 Super Scan 的应用

Super Scan 是功能强大的端口扫描工具，它具有以下功能：掌握个人计算机的 IP 情况，进行 IP 和域名的相互转换，通过 Ping 来检验 IP 是否在线；IP 和域名相互转换；检测所有端口；自定义要检验的端口，并可以保存为端口列表文件；通过木马端口列表 trojans.lst 检测目标计算机是否有木马。本书只对此端口扫描工具的部分功能进行介

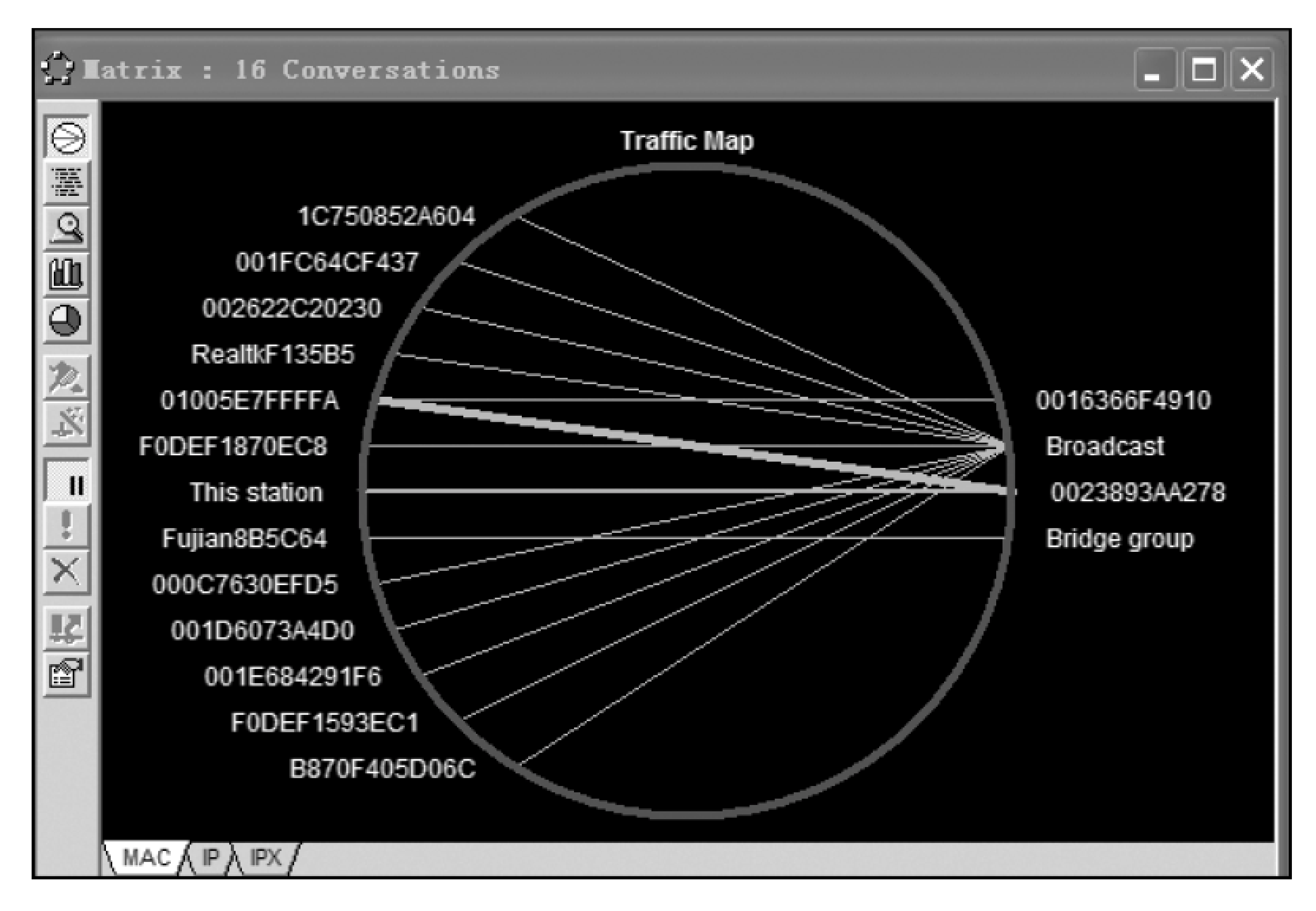


图 8-27　本机与网络其他地址的流量图

绍。下面介绍如何在个人计算机使用端口扫描工具检测网络使用状况。

1．安装 Super Scan 软件

Super Scan 是一款绿色软件，直接解压下载后的程序包就可安装，安装成功，可以看到软件主界面如图 8-28 所示。

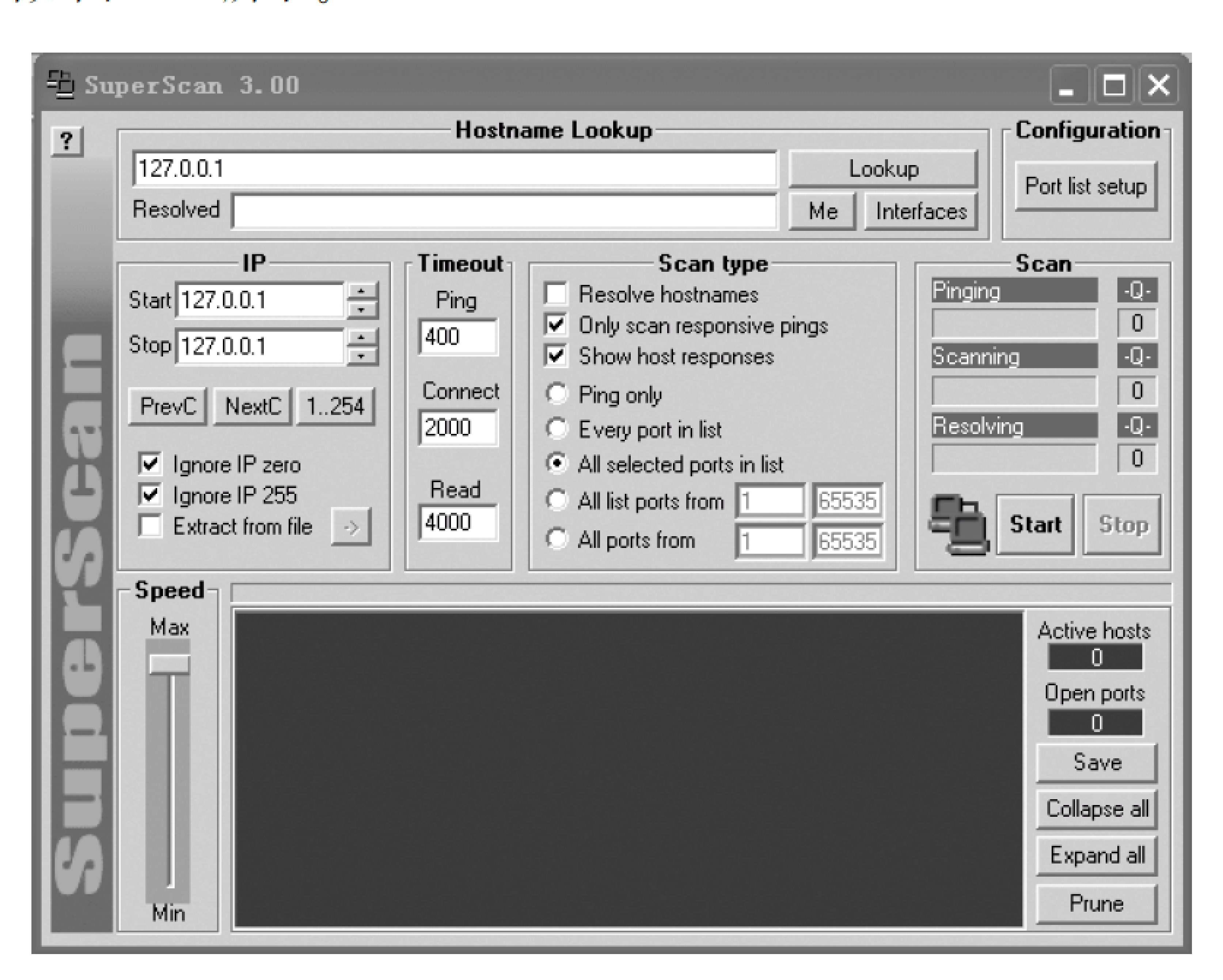


图 8-28　Super Scan 主界面

2．掌握自己计算机的 IP 情况

第 1 步：取得自己计算机的 IP。

单击图 8-28 中的“Hostname Lookup”框中的【Me】按钮来取得。

第 2 步，取得自己计算机的 IP 设置情况。

单击图 8-28 中的“Hostname Lookup”框中的【Interfaces】按钮，取得本地 IP 设置情况，如图 8-29 所示。

3. 域名(主机名)和 IP 相互转换

方法一：通过“Hostname Lookup”实现。

第 1 步：在图 8-28 中“Hostname Lookup”框中的【Lookup】左边的空白输入栏中输入需要转换的域名或者 IP。

第 2 步：单击图 8-28 的【LookUp】按钮，实现转换。

方法二：通过 “Extract from file”实现。

第 1 步：勾选位于图 8-28 左边中间位置的“Extract from file”选项。

第 2 步：单击“Extract from file”选项后的【—>】按钮，选择域名列表，出现如图 8-30 所示的转换向导图。

第 3 步：实现转换。

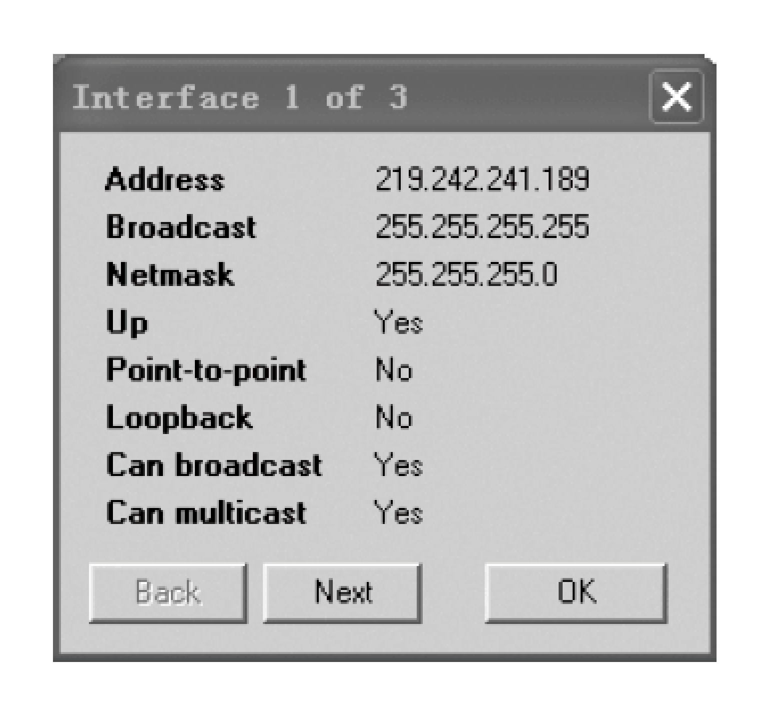


图 8-29　本地 IP 设置情况

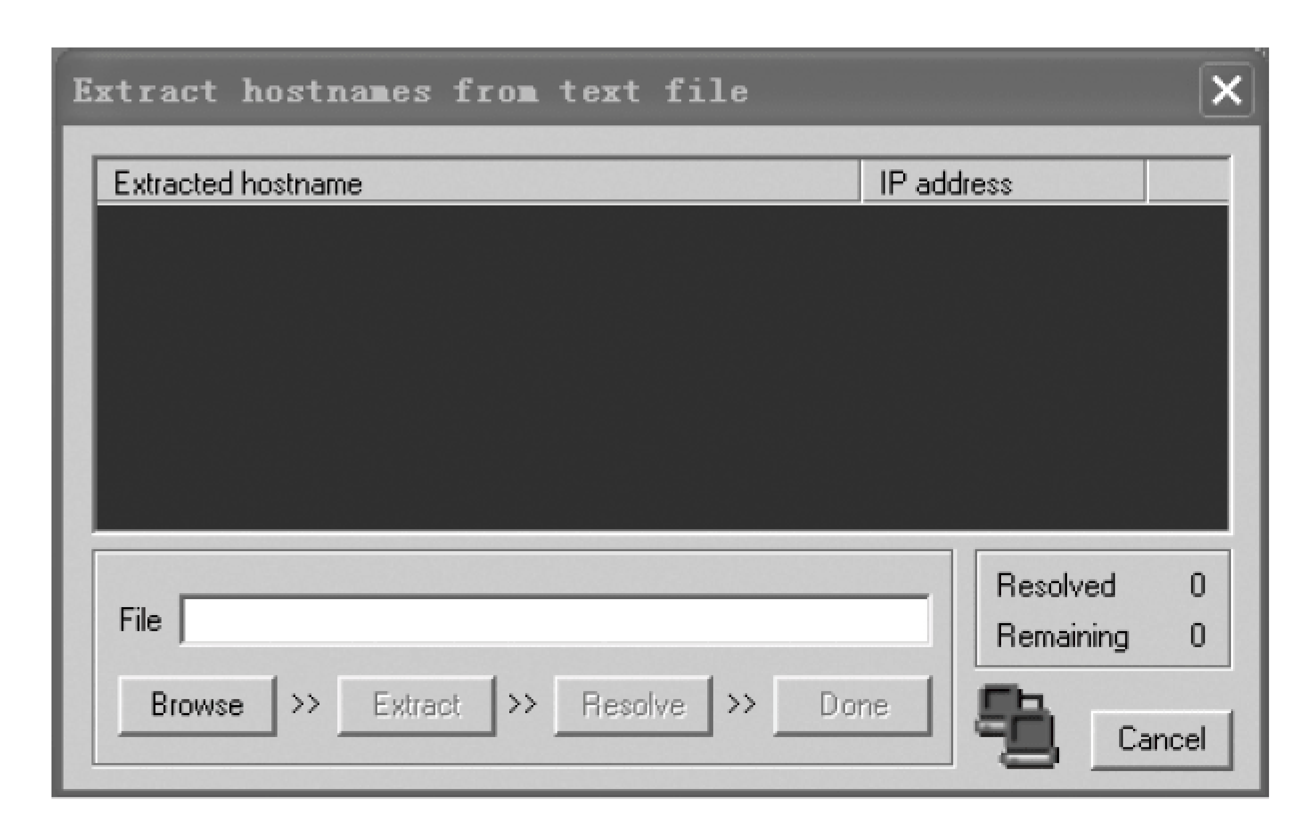


图 8-30　转换向导图

4. Ping 功能的使用

第 1 步：输入 IP。

在图 8-28 中“IP”框中的“Start”栏中填入起始 IP，在“Stop”栏中填入结束 IP。

第 2 步：进行检测。

(1) 选择图 8-28 中间位置的“Scan type”对话框里的“Ping only”选项，再单击位于右边的【Start】按钮进行检测。

(2) 图 8-31 中的蓝屏区域为检测结果，蓝屏区域中的 IP 地址前是“√”代表此 IP 地址的目标计算机在线，IP 地址前是“×”则的代表此 IP 地址的目标计算机不在线。从图 8-31 可以看出，IP 地址为 219.242.240.2 的目标计算机不在线。

在进行检测时，为了达到方便快捷，可以利用以下按钮达到快捷设置的目的，其中快捷键有：

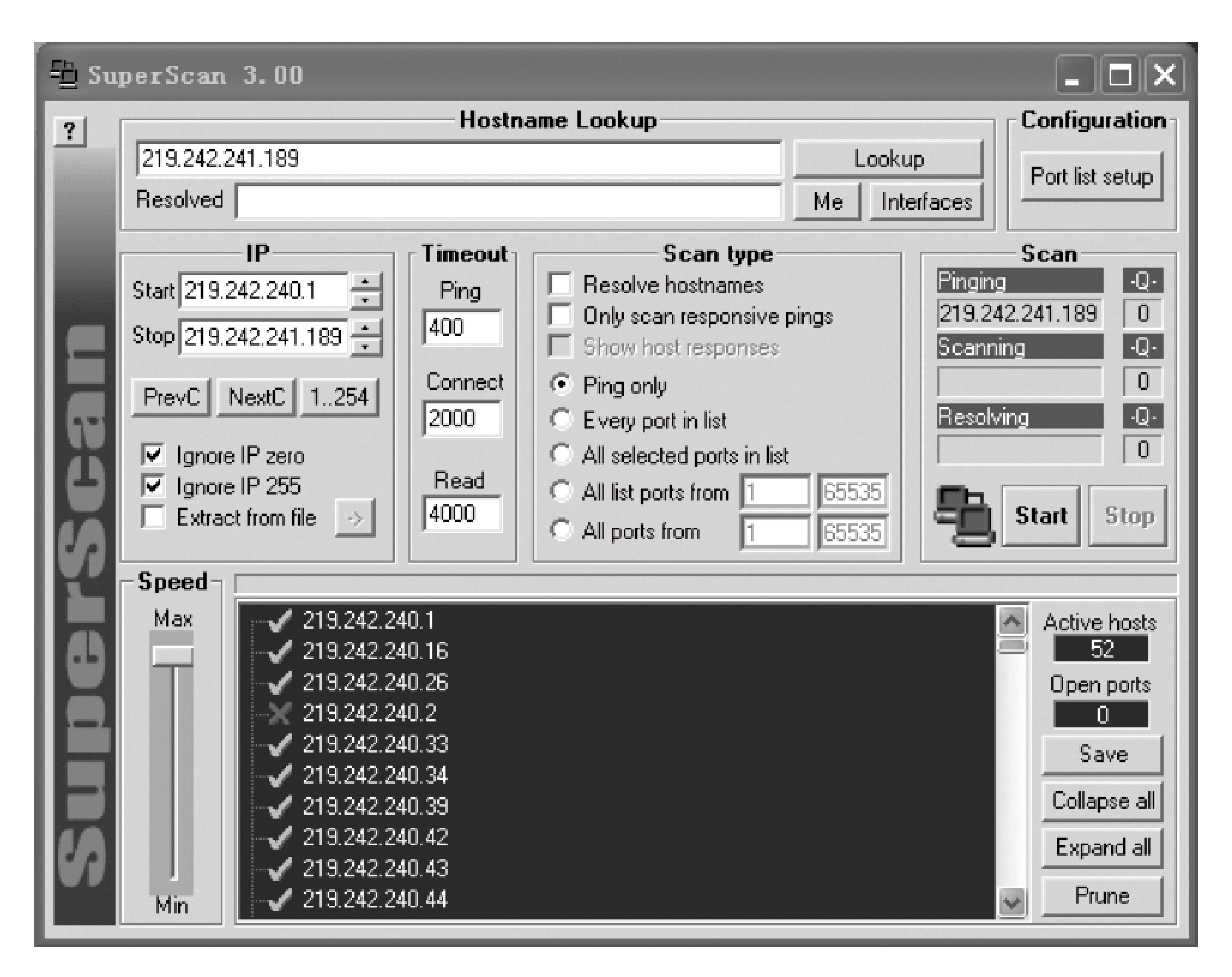


图 8-31　Ping 功能检测结果

① 【Ignore IP zero】：屏蔽所有以 0 结尾的 IP；

② 【Ignore IP 255】：屏蔽所有以 255 结尾的 IP；

③ 【PrevC】：直接转到前一个 C 网段；

④ 【NextC】：直接转到后一个 C 网段；

⑤ 【1..254】：直接选择整个网段。

⑥ 【Extract from file】：通过域名列表取得 IP 列表。

5. 检测所有的端口

第 1 步：输入要检测的 IP 地址范围。

（1）在图 8-28 中的“IP”框中的“Start”栏中填入起始 IP，在“Stop”栏填入结束 IP。

（2）选择图 8-28 中间位置的“Scan Type”框中的“All ports from”选项。

第 2 步：单击【Start】按钮进行检测。

第 3 步：查看扫描结果。

（1）单击图 8-28 中右下方的【Expand all】按钮，查看扫描的结果，如图 8-32 所示。

（2）图 8-32 的蓝色区域是检测目标计算机所有端口的结果。第一行是目标计算机的 IP 和主机名；从第二行开始的小圆点是扫描的计算机的活动端口号和对该端口的解释。蓝色区域右方的“Active hosts”标签下的方框显示扫描到的活动主机数量，为 52；“Open ports”标签下的方框显示目标计算机打开的端口数，这里是 2。

此种检测适应于为了了解目标计算机的详细情况，一般不提倡这种检测，因为：它会对目标计算机的正常运行造成一定影响，同时，也会引起目标计算机的警觉；扫描时间很长；浪费带宽资源，对网络正常运行造成影响。

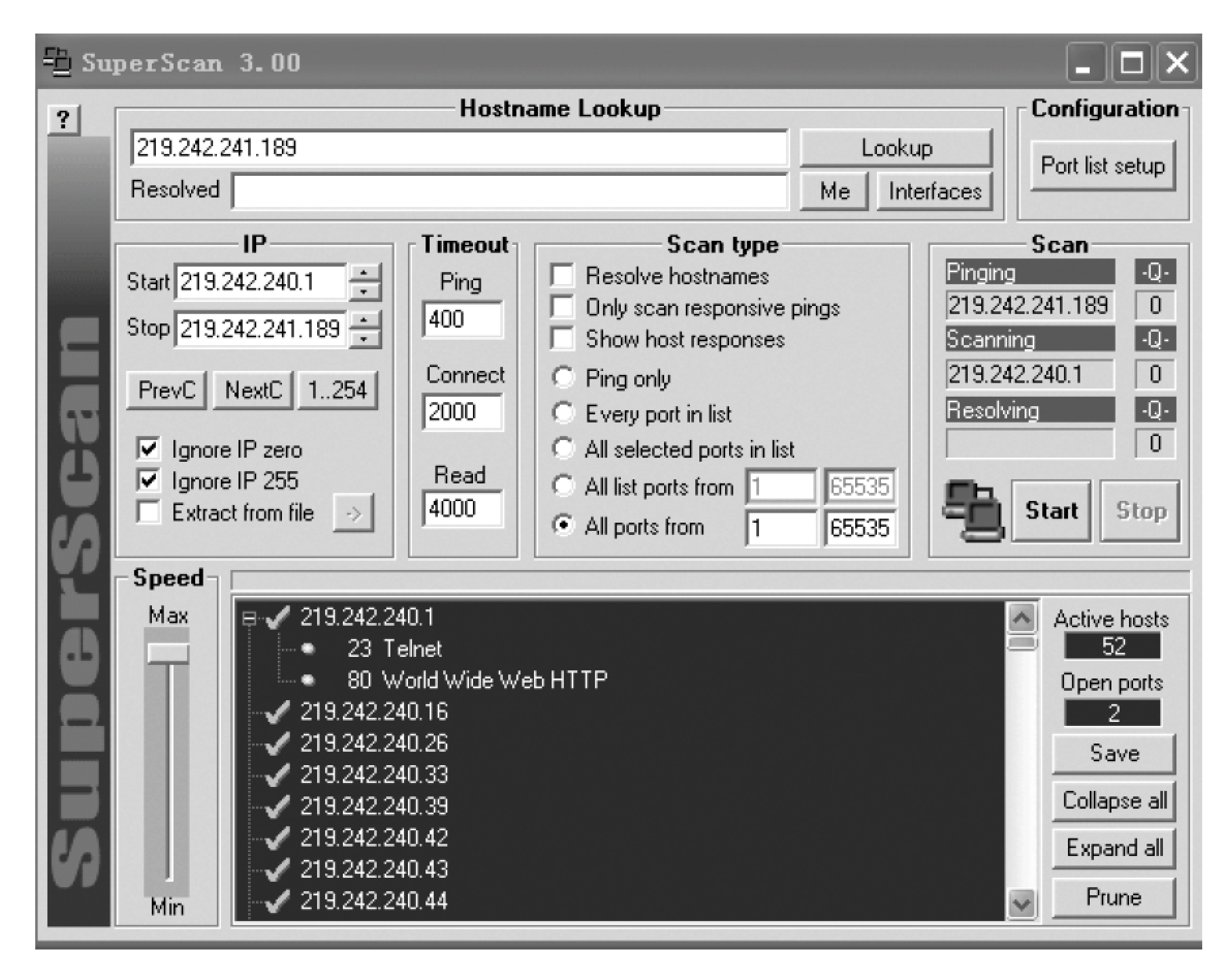


图 8-32　所有端口的扫描结果

8.4.3　360 安全卫士木马防火墙的应用

360 安全卫士防火墙是一款保护用户上网安全的产品，它通过一系列安全设置，例如安全防护状态的设置，信任列表的设置，阻止列表的设置，防护日志的设置和防火墙规则设置等来阻截各类网络风险，使用户能方便地使用安全网络。下面介绍如何在个人计算机中使用 360 安全卫士。

1. 安装 360 安全卫士

安装好 360 安全卫士后，运行 360 安全卫士，进入 360 安全卫士功能大全界面，如图 8-33 所示。

2. 安全防护状态设置

第 1 步：进入 360 木马防火墙界面。

(1) 单击图 8-33 中的“360 安全产品”标签，进入 360 安全产品界面，如图 8-34 所示。

(2) 单击图 8-34 中的 “360 木马防火墙”标签，进入“360 木马防火墙”对话框，如图 8-35 所示。

第 2 步：设置安全防护。

(1) 图 8-35 中防护状态框中的上网安全防护已开启。

(2) 单击上网安全防护的【已开启】按钮，会出现提示信息要关闭上网安全防护，如图 8-36 所示。



图 8-33　360 安全卫士功能大全



图 8-34　360 安全产品



图 8-35 “360 木马防火墙”对话框

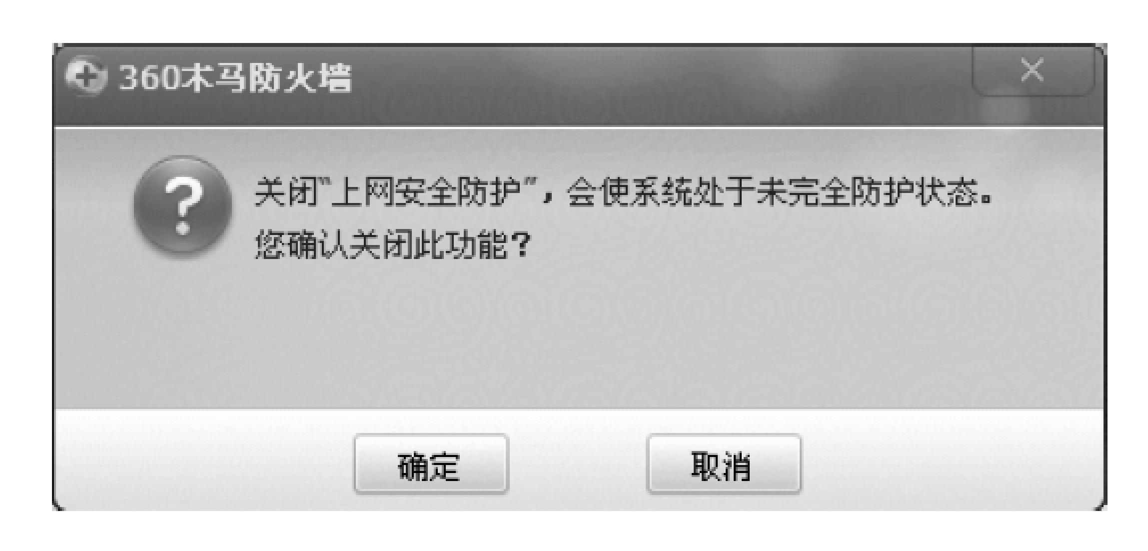


图 8-36 上网安全防护关闭警告

（3）单击图 8-36 中的【确定】按钮，则关闭上网安全防护，若单击【取消】按钮。则不关闭上网安全防护。

按照上述操作根据个人的安全需要修改各项防护状态。

3. 信任列表设置

第 1 步：进入信任列表界面。

单击图 8-35 中的“信任列表”标签，进入“信任列表”对话框，如图 8-37 所示。

第 2 步：设置信任选项。

单击图 8-37 中的“信任列表”对话框右下方的【添加信任】按钮，会出现选择信任程序对话框，如图 8-38 所示。

根据个人需要在计算机中选择要执行的文件，本书以 D:\下载软件\QQmusic2011.exe 为例，将其加入信任列表，会显示图 8-39 所示的结果。



图 8-37 信任列表对话框

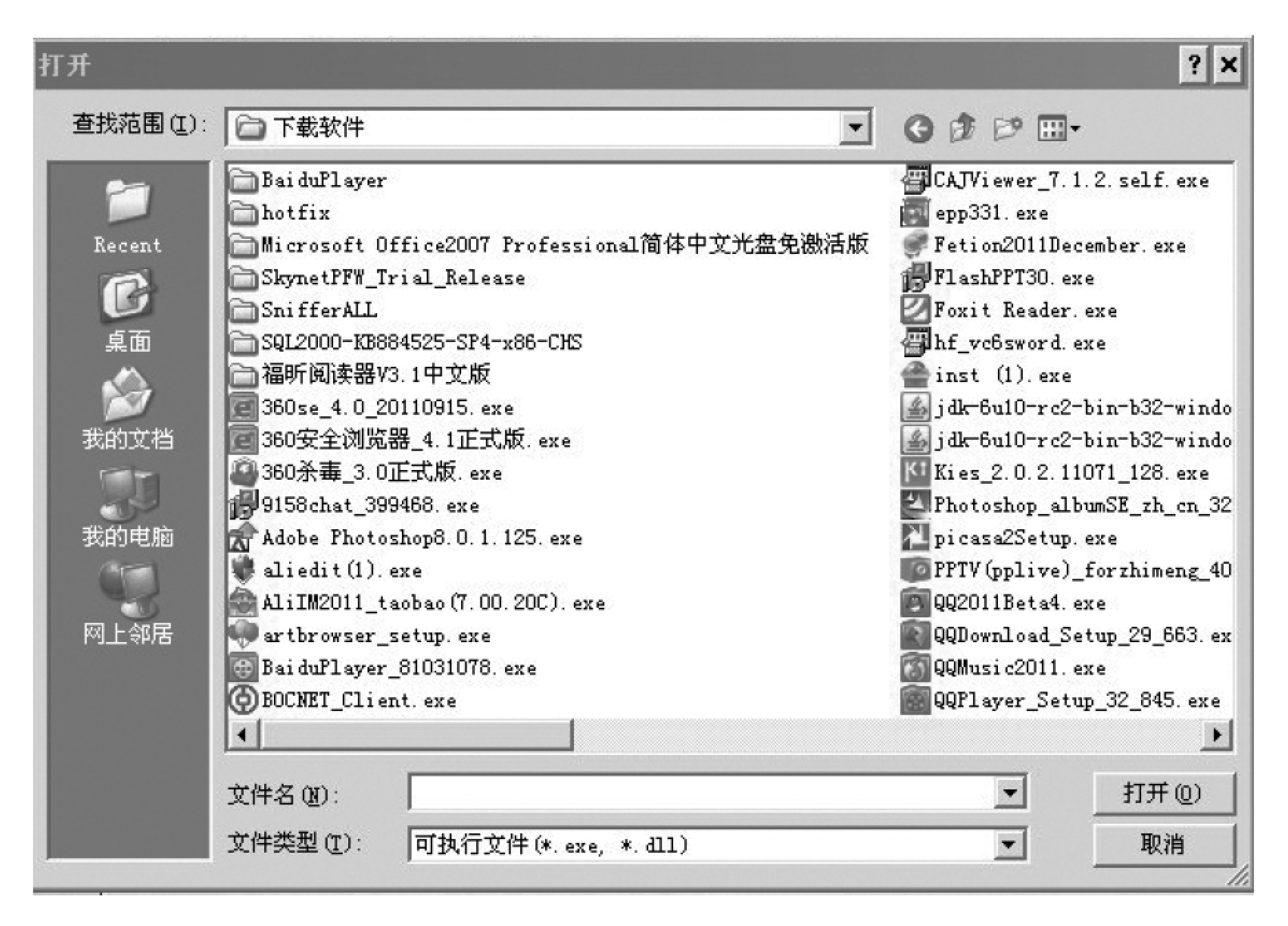


图 8-38 选择信任程序对话框

图 3-39 所示的界面表示添加已经成功，若想取消此添加，单击图 8-39 信任文件后面的“移除”标签，则添加取消。

第 3 步：设置信任列表。

根据个人需要按照第 2 步的操作重复进行需要添加的信任，完成信任列表。若要进



图 8-39 添加信任程序成功结果显示

行多个程序的删除，可以选中需要删除的信任程序，然后单击【清空已选程序】按钮。

4. 阻止列表的设置

设置阻止列表的操作与设置信任列表的操作类似，本书不再做详细介绍。

5. 防护日志的设置

第 1 步：进入防护日志界面。

单击图 8-35 中的“防护日志”标签，打开防护日志对话框，如图 8-40 所示。

第 2 步：查看防护日志。

单击图 8-40 中的“系统防护日志”标签，并勾选“防护日志”对话框左下方的“显示全部日志”选项，在防护日志对话框的空白处显示系统防护的全部工作记录，如图 8-41 所示。

第 3 步：修改防护日志。

单击图 8-41 中的【清空所有日志】按钮可以删除防护日志。

第 4 步：保存防护日志。

根据个人需要，选择防护记录，再单击图 8-41 下方的【复制选中内容】按钮，对选中防护记录进行复制，最后进行保存。若想全部进行保存，可以直接单击【复制全部内容】按钮。

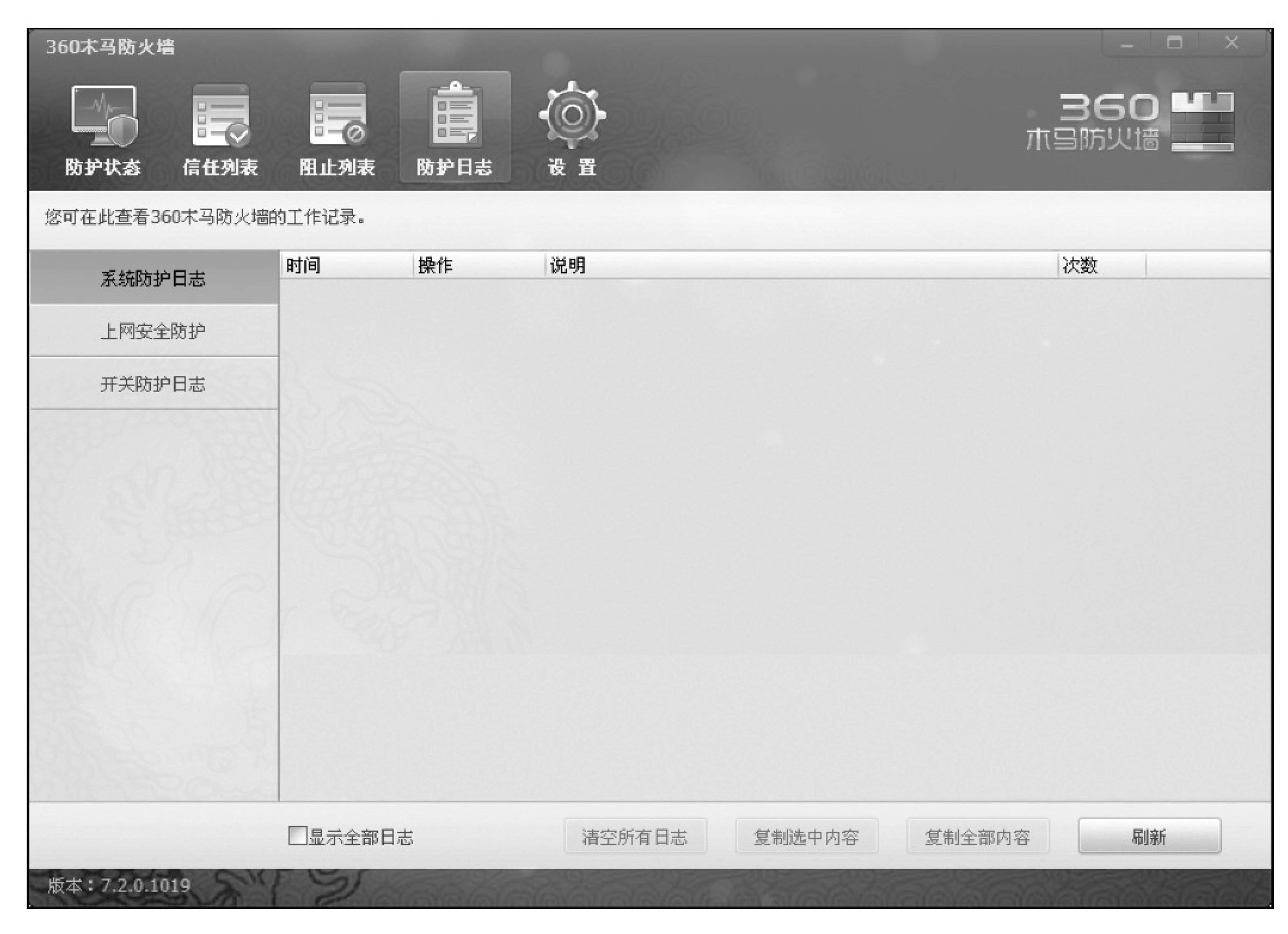


图 8-40　防护日志对话框



图 8-41　系统防护日志

6. 防火墙规则的设置

第 1 步：进入设置防火墙规则对话框。

单击图 8-35 中的“设置”标签，打开防火墙规则设置操作框，如图 8-42 所示，根据个人安全需要可以对入口防御、隔离防御、系统防御、应用防护、高级设置进行规则设置。本书以入口防御规则设置为例。



图 8-42　防火墙规则设置操作框

第 2 步：设置入口防御规则。

(1) 单击图 8-42 中的“入口防御”标签，出现入口防御规则设置操作框，如图 8-43 所示，根据个人需要勾选“防护项目”框中防护选项。

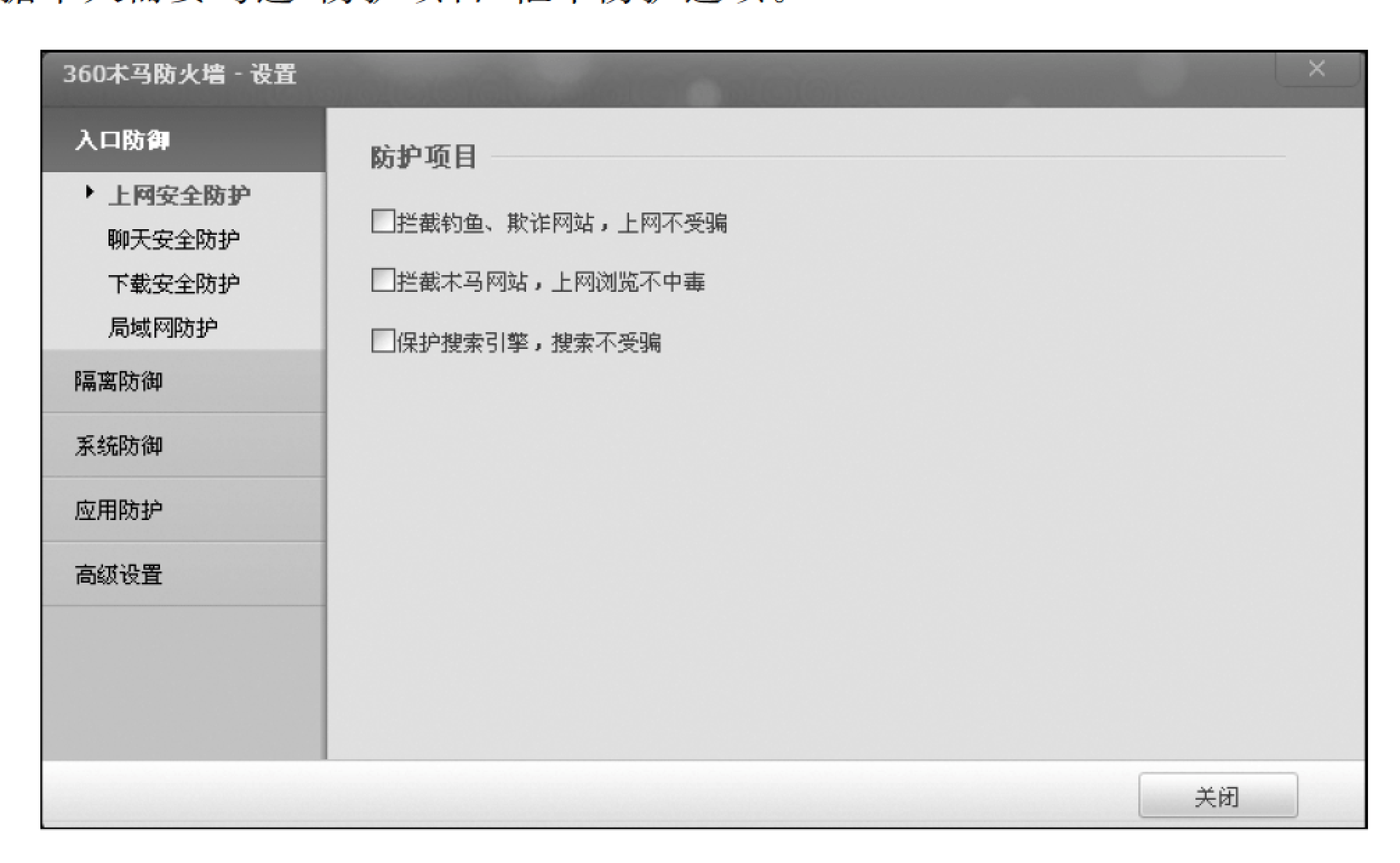


图 8-43　入口防御规则设置操作框

（2）设置完成后，单击【关闭】按钮退出设置。

其他防御设置类似。可按照上述的操作根据个人需要进行防御规则的设置。

8.5 案例讨论

2009 年微软公司旗下 Hotmail 电子邮箱 1 万个账户信息于 10 月 1 日在一家计算机专业网站上被曝光。随后网上又出现一份包含 2 万个电子邮箱账户地址及密码的清单，这些邮箱所属包括微软、谷歌、雅虎、美国在线等主要电邮服务商。

事件发生后，微软公司在一份声明中说："我们知道一些 Hotmail 用户的通行证遭'网络钓鱼'非法窃取并被公布在网站上，我们立即要求移除这些通行证并展开调查，确认这不是微软服务器的漏洞，随后我们采取措施阻止登录这些失窃账户，帮助用户再建账户。"

谷歌公司 6 日发表声明说："我们得知这次袭击后，立即对失窃账户强制重置密码，我们将继续对更多账户强制重置密码，直至调查清楚。"

"网络钓鱼"是一种利用网络骗取用户个人信息的程序。黑客通常利用这种程序假扮成享有信誉的公司，如银行或在线商店向用户索要账户名及密码等信息。

"网络钓鱼攻击几乎不可能阻止，"英国前进网络集团首席技术官员卢卡斯·奥伯胡贝尔说，"因为他们使受害者相信将私人信息提供给一个安全网站，骗子一直做的就是骗取人们信任。"

奥伯胡贝尔还说："网络钓鱼已持续很多年，所以这种危害并不令人吃惊，这种攻击愈加狡猾，所有最新版的主要网络浏览器都带有防钓鱼程序，但问题是，这种程序对浏览器不知道的钓鱼网站不起作用。"

讨论网络钓鱼攻击的危害，说明在实际使用网络时应该如何防范网络钓鱼？

归纳总结

1. 通过本章内容，可以看出网络应用关系到我们生活的方方面面。归纳总结作为一个网络使用者，需要从哪些方面提高网络应用安全的警惕性。

2. 归纳总结个人在使用网络应用时应该采取哪些安全措施。

3. 归纳网络钓鱼与网络肉鸡的危害，总结有哪些类型的网络应用安全技术。

思考与实践

思考题

1. 网络应用安全的威胁有哪些？各有什么危害？

2. E-mail 的工作原理是什么？目前电子邮件主要有哪些安全漏洞与威胁？

3．什么是网上支付？网上支付的工具有哪些？

4．网络钓鱼的主要方式有哪些？能从哪些方面进行防范？

5．网络监听的概念是什么？网络监听的防范措施有哪些？

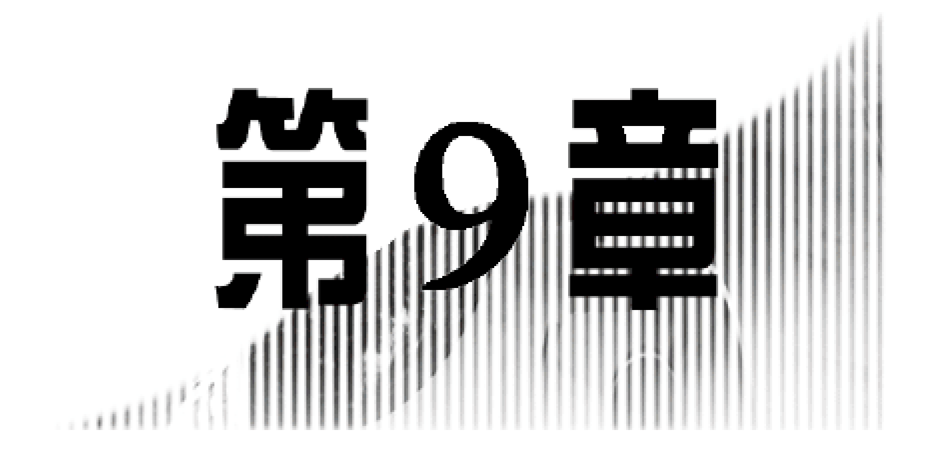
6．端口扫描的原理是什么？其防范措施有哪些？

实践题

1．请使用其他的网络监测软件进行网络监测，并说明其与 Sniffer Pro 网络监测软件的区别。

2．对个人计算机进行本书中未详细介绍的 Super Scan 的其他相关功能的使用，例如扫描特定端口或通过木马端口列表 trojans. lst 检测目标计算机是否有木马等。

3．请设置应用实例中 360 安全卫士防火墙中 360 流量防火墙规则。



应急响应与灾难恢复

学习目标

通过本章的学习，能够——

- 了解应急响应与灾难恢复的含义；
- 了解容灾与数据备份的方法和技术；
- 了解应急响应的组织与程序；
- 了解灾难恢复的策略与步骤；
- 掌握 Ghost 和 Winhex 的基本使用方法。

引导案例

美国东部时间 2001 年 9 月 11 日上午，四架美国国内民航航班几乎被同时劫持，其中两架撞击位于纽约曼哈顿的世界贸易中心。9·11 恐怖袭击事件已经过去 10 年有余，但它带给世人的影响却远没有过去，甚至成为许多人心中永远的痛。此次恐怖袭击不仅造成两栋 400 米摩天大厦的坍塌，使 2998 余名无辜者不幸罹难，还彻底毁灭了数百家公司所拥有的重要数据。在此次灾难之后的废墟中，深埋着 800 多家公司和机构的重要数据，其中许多公司的数据，特别是那些没有进行备份的数据，永远无法恢复了。坐落在纽约的世贸中心，曾经是美国乃至全球财富的象征，在这座建筑群中，聚集了众多全球一流的大公司，不少是银行、证券和 IT 行业的翘楚，如世界著名的摩根-斯坦利公司、AT&T 公司、SUN 公司、瑞士银行等。在 9·11 恐怖袭击事件中，这些世界金融和 IT 的巨头也遭受了不同程度的损失。

国外的一项调查表明，因灾难而丢失关键数据，并且在几天内不能恢复关键业务的企业将会从市场上消失。对于依赖计算机系统运作的金融、电信、保险、民航、铁路和制造业而言，系统停机的可忍受时间更短。

如果大家觉得恐怖袭击造成的灾难离我们很遥远，那么下面的事情可是发生在我们身边。

2008 年初春中国南方遭遇一场历史罕见的冻雪灾害，大面积的冻雪压垮了南方多个省市的电网，造成大范围电力系统和铁路行车信号控制系统瘫痪。大批客货列车停运，高

速封闭，多座城市陷入黑暗之中。这其中不仅造成大批人员伤亡，而且带来了巨大的经济损失。很多企业的信息系统不能运行，造成公司经营业绩下降或运营瘫痪。

随着信息系统的普及，信息化已成为必然的趋势，并深入人们生活的方方面面。如何应对系统运行中诸如灾难带来的危害，是当今个人、企业乃至全社会亟待解决的问题。

9.1 应急响应与灾难恢复概述

随着信息化浪潮不断袭来，我们正在逐步走进信息时代。毫无疑问，信息技术的广泛应用给人类生活带来了空前的便利享受。但是在便利的背后计算机的运行安全却面临严重威胁，一旦遭受信息灾难，带来的损失是无法预计的。所以做好应急响应与灾难恢复工作是企业运营中不可或缺的环节。

本节主要介绍信息灾难的含义、信息灾难的威胁与防范信息灾难的技术。

9.1.1 应急响应与信息灾难的含义

过去人们依赖交易员的手工操作来进行股票买卖，如今只要在一台联网的计算机上甚至是联网的手机上即可完成股票交易。过去通过慢速昂贵的人工手段传递信息，如今依靠电子邮件和电话就能方便联系。俗话说："任何事物都有两面性。"很难想象，如果电子交易系统、电子邮件和电话系统等突然中断，人们的反应将如何。如果银行、医疗和武器系统控制软件出现故障，将会有何种后果？

1. 应急响应

应急响应(incident response/emergency response)通常是指一个组织为了应对各种安全事件的发生所做的准备工作以及在突发事件发生时或者发生后所采取的措施。

这里的"安全事件"是指破坏数据与信息系统的行为。包括：

(1) 保密性安全事件。例如入侵系统并读取信息、搭线窃听、远程探测网络拓扑结构和计算机系统配置等。

(2) 完整性安全事件。例如入侵系统并篡改数据、劫持网络连接并篡改或插入数据、安装特洛伊木马、计算机病毒(修改文件或引导区)等。

(3) 可用性安全事件。例如系统故障、拒绝服务攻击、计算机蠕虫(以消耗系统资源或网络宽带为目的)等。

应急响应的对象是指计算机或网络所存储、传输、处理的信息的安全事件，事件的主体可能来自自然界、系统自身故障(这里的系统包括主机范畴内的问题，也包括网络范畴内的问题)、组织内部或外部的人、计算机病毒或蠕虫等。

2. 灾难的含义与后果

灾难指由于自然的原因(洪水、台风、地震、雷击等)，意外事故(火灾、塌方、供电故障)，恶意攻击，人为失误等造成信息系统运行严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定时间的突发性事件，通常导致信息系统需要切换到

备用场地运行。

从业务连续性角度进行观测，灾难的后果会造成计算机信息系统与基础设施中断，进而导致业务流程中断。这种中断包括如下几种现象：

① 网络中断(通信链路失效)；

② 信息系统中断(节点失效)；

③ 硬件和软件模块故障(组件失效)；

④ 数据本身损毁(数据失真)。

从更广泛的范围来看，灾难会导致计算机信息系统与基础设施遭到损坏，具体来说包括如下几种现象：

① 数据毁损(失真、被毁)；

② 系统中断(暂停、死机、崩溃)；

③ 系统错误(服务继续，但服务有误)；

④ 系统恶变(系统性质逆转)；

⑤ 基础设施毁坏。

1970 年越南战争期间，美国威斯康星大学的国防数学研究中心遭到炸弹袭击(如图 9-1 所示)。结果是一个研究生被杀害，整个建筑被炸，计算机信息系统与积累了 20 年的数据全部毁于一旦。9·11 恐怖袭击事件更是使入驻世贸中心(如图 9-1 所示)的几百家公司数据瞬间被毁，造成许多公司无法继续运营。




图 9-1　被炸毁的国防数学研究中心与世贸中心

3. 灾难的类型

灾难通常分为两大类：数据灾难和系统灾难。

(1) 数据灾难。

数据灾难指的是灾难造成数据不能正常使用。数据灾难可以分为三种情况：

① 数据失真，即数据的内容发生错误；

② 数据部分丧失，即部分数据不能使用；

③ 数据完全被毁，即整个数据系统无法再使用。

(2) 系统灾难。

系统灾难指的是运行处理数据的信息系统本身因灾难打击无法正常运行。系统灾难可以分为三类：

① 系统失灵，即系统仍在运行，但出现行为错误，如飞机在处于危险情况中，并未发出危险警报；

② 系统瘫痪，即系统完全停止工作；

③ 系统恶变，即系统仍在运行，但运行的结果是随机的甚至完全相反的。例如，当敌人入侵时，雷达未能发出警报甚至是被敌人控制用来对付自己。

9.1.2 应急响应组织的产生与发展

1. 应急响应组织的产生

应急响应源自于1988年莫里斯蠕虫案件。该案件轰动了全世界，并且在计算机科学界引起了强烈的反响。此案标志着大众对计算机网络所产生的脆弱性的突然警醒。蠕虫发作后全美国一片慌乱的情景，使人们前所未有地认识到，随着人们对计算机的依赖日益加深，与此同时计算机网络遭受攻击的可能性也在增大。随着计算机之间联系越来越紧密，随着网络对越来越多的人开放，出现莫里斯蠕虫一类的程序其实是不可避免的。尽管如此，当这样的程序到来时，人们还是感到极大的震惊。为此，1989年，美国国防部高级研究计划署资助卡内基·梅隆大学建立了世界上第一个计算机紧急响应小组（computer emergency response team，简称CERT）及协调中心（CERT/CC）。CERT的建立标志着信息安全由传统的静态保护手段开始转变为较为完善的动态防护机制。

2. 应急响应组织的发展

随着互联网的飞速发展，出于对网络安全的需要，国际上先后成立了一大批的应急响应组织（computer security incident response team，简称CSIRT）。例如美国联邦FedCIRC，德国的DFNCERT，以及亚太地区APCERT和欧洲EuroCERT。1990年成立了一个应急响应与安全组论坛FIRST（forum of incident response and security teams），发起时有11个成员，至2002年初已经发展成一个超过100个成员的国际性组织。据粗略统计，目前已建立应急处理机制的国家和地区已达60多个，应急组织的总数则超过了200多个。

3. 中国应急响应的组织

在世界上第一个计算机应急响应小组及协调中心成立后十年，中国也开始陆续建立起应急响应机构，教育与科研计算机网于1999年在清华大学成立CERNET应急响应组（CCERT），为中国教育和科研行业用户提供应急响应服务。2000年10月，国家计算机网络应急技术处理协调中心（CNCERT/CC）成立，并于2002年8月成为国际应急响应权威组织“事件响应与安全组织论坛（FIRST）”的正式成员。在CNCERT/CC的协调组织下，中国电信、中国网通、中国移动等各大电信运营商都纷纷成立自己的应急响应队伍。

随后解放军军队应急组织、公安部计算机病毒防治中心、公安部计算机应急网站也先后建立,并且许多公司也都展开了网络安全救援相关的收费服务。此外,还成立了一些专业性的应急组织,如国家计算机网络入侵防范中心、国家863计划法计算机入侵和防病毒研究中心等。

4. 应急响应组织所提供的服务

世界各国的应急响应机构所提供的应急响应服务基本相同,主要包括以下几个方面的内容:

(1) 提供应急响应服务;
(2) 提供安全咨询服务;
(3) 提供系统评估或风险评估服务;
(4) 提供入侵检测服务;
(5) 发布安全公告;
(6) 发布漏洞信息;
(7) 提供补丁下载;
(8) 教育与培训;
(9) 追踪与恢复;
(10) 组织各种形式的学术交流活动。

9.1.3 灾难发生的原因与危害

1. 灾难发生的原因

造成灾难的原因有自然因素,如火灾、洪水、地震、飓风、龙卷风、台风等,还有其他如原先提供给业务运营所需的服务中断,如设备故障、软件错误、电信网络中断和电力故障等。此外,人为的因素往往也会酿成大祸,如操作员错误、破坏、植入有害代码和黑客攻击。现阶段,由于我国很多行业正处在高速发展的阶段,很多生产流程和制度仍不完善,加之缺乏经验,导致灾难也屡见不鲜。

经过统计分析发现,导致灾难硬件故障原因占44%,人为错误原因占32%,软件故障原因占14%,病毒影响原因占7%,自然灾难原因占3%。

2. 灾难的危害

灾难会对使用信息系统和计算机的机构或个人造成各种程度的伤害。轻则导致财产损失,重则造成人员伤亡。也可能造成企业业务停顿、利润下降、信誉受损、公司破产甚至可能导致政府危机、垮台等。例如,9·11事件一年后,重返世贸大厦的企业由原来的350家减少到150家,200家企业由于重要信息系统的破坏及关键数据的丢失永远的倒闭消失了。

根据互联网数据中心的调查,在20世纪最后10年中,在美国发生过灾难的公司中,55%的公司当即倒闭,剩下45%中,因为信息数据丢失,其中29%的公司在两年内

倒闭,能生存下来的仅占16%。根据美国劳工部的统计数据,在丢失关键数据记录的公司里,90%的公司在1年内破产。对于那些丢失重要数据记录的公司来说,其利润将下降30%～50%!

由此可见,加强对信息系统的保障在灾难面前显得尤为重要。因此,各国都对信息系统的灾难恢复工作十分重视,并采取了积极的应对措施。

9.1.4 容灾和灾难恢复

在9·11事件中,随着大厦的轰然坍塌,无数人认为摩根-斯坦利将成为这一恐怖事件的殉葬品之一。然而,正当大家为此扼腕痛惜时,该公司竟然奇迹般地宣布,全球营业部第二天可以照常工作。摩根-斯坦利公司之所以能够在9月12日恢复营业,其主要原因是它不仅像一般公司那样在内部进行数据备份,而且在新泽西州建立了灾备中心,并保留着数据备份。9·11恐怖袭击事件发生后,摩根-斯坦利公司立即启动新泽西州的蒂内克的灾难备份中心,从而保障了公司全球业务的不间断运行,有效降低了灾难对于整个企业发展的影响,同样进行了异地数据备份的还有JP摩根、瑞宝银行以及雷曼兄弟等公司,他们也在9月12日恢复了营业,而很多没有建立灾难备份系统的企业却没有这样幸运。

通过这次事件,人们开始意识到容灾和灾难恢复技术的重要性。

1. 容灾技术

不管如何小心防范,总会有一些意想不到的灾难发生。灾难来临,意味着可能发生风险。但是如果提前预警,提前知道灾难可能发生以及灾难发生后的结果,有针对性地采取应对措施,就可以减轻灾难造成的损失,因此,产生了容灾的理念。

容灾对于计算机信息系统而言,就是提供一个能防止用户业务系统遭受各种灾难破坏与攻击影响的系统。容灾还表现为一种未雨绸缪的主动性,不是在灾难发生后的"亡羊补牢"。

从狭义的角度讲,容灾是指除了生产站点以外,用户另外建立的冗余站点,当灾难发生,生产站点受到破坏时,冗余站点可以接管用户正常的业务,达到业务不间断的目的,业务连续性是容灾的最终建设目标。

2. 灾难恢复

(1) 灾难恢复的含义

灾难恢复是将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态,并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设计的活动和流程。

灾难恢复与普通数据恢复的最大区别在于:在整个系统都失效时,用灾难恢复措施能够迅速恢复系统而不必重装系统。

(2) 灾难恢复技术的发展。

从20世纪70年代至今,灾难恢复技术大致经历了三个发展阶段:第一个阶段是在20世纪90年代之前,主要关注如何恢复数据和信息系统;第二个阶段从20世纪90年代

到2000年左右，主要关注如何恢复支撑业务，并从业务的角度评估业务的关键程度，以及业务恢复的范围和恢复指标；2000年后，进入到第三阶段，以保障机构长期、持续、稳定地运行为目的，从管理的角度来看待灾难恢复和业务连续。

(3) 灾难恢复系统。

灾难恢复系统是为了保障计算机系统和网络系统在发生灾难的情况下，能够迅速地得以恢复原来状态而特意建立的一整套完整的系统，它是灾难恢复技术的集中体现，它具有系统备份、可重置路由的数据通信线路、电源以及数据备份等功能，还包含应急预案等内容。其中，系统备份与数据备份的不同在于，它不仅仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便需要时迅速恢复整个系统。

此外，灾难恢复系统还包括对系统的定期测试和使用人员的培训，以保证参与灾难恢复系统的人们能够更好地对灾难的发生做出合理的反应。

9.2 应急响应模型与操作流程

建立完善的计算机应急响应系统，其任务不应该仅仅局限于建立一个用于提供应急响应和发布安全公告的信息中心，而应该把系统置身于各种具体的安全事件、安全问题、安全技术之上，从全局的角度建立一个具备合理的组织架构、高效的信息流程和控制流程、完备的安全研发及服务体制、长远的实施和发展规划、丰富的信息来源，以及良好的国际国内合作协调关系的大范围的、分布的、动态的安全保障系统。

本节主要介绍应急响应模型与应急响应的操作流程。

9.2.1 应急响应模型

1. PDRR 应急响应模型

在研究信息安全及网络战防御理论的过程中，美国国防部提出了信息保障(information assurance，IA)的概念，并给出了包含防护(protection)、检测(detection)、响应(response)3个环节的动态模型，后来又增加了恢复(restore)环节，简称为PDRR模型，如图9-2所示，其中的响应环节包括平时事件响应和应急响应，重点在于针对安全事件的应急处理。

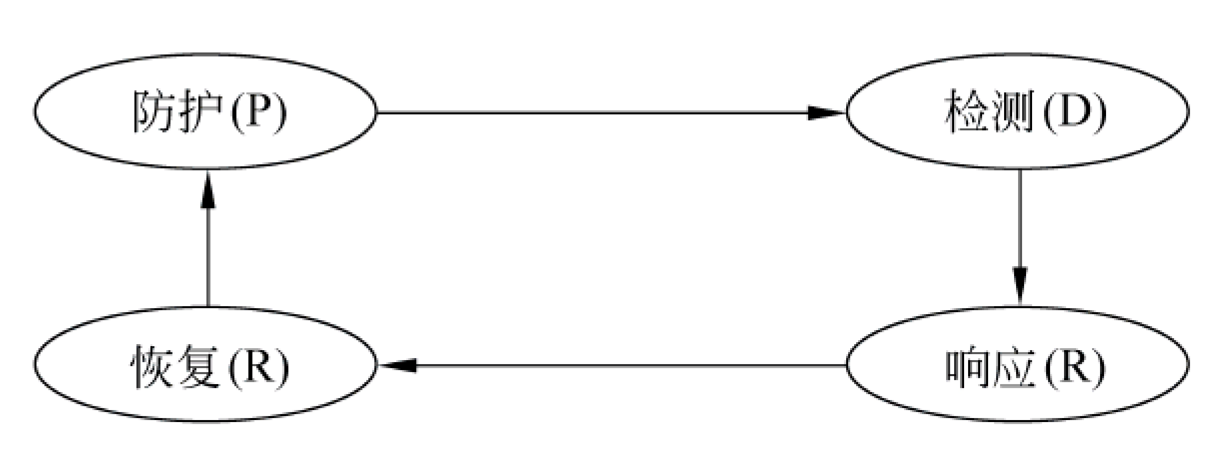


图9-2　PDRR网络安全模型

PDRR 模型的第一部分就是防护。根据系统已知的所有安全问题做出防护的措施，如打补丁、访问控制、数据加密等。防护作为 PDRR 模型的第一个战线。

PDRR 的第二个战线就是检测。攻击者如果穿过了防御系统，检测系统就会检测出来。这个安全战线的功能就是检测出入侵者的身份，包括攻击源、攻击状况、系统损失等。

一旦检测出入侵，响应系统开始响应包括事件处理和其他业务。

PDRR 模型的最后一个战线就是系统恢复。在入侵事件发生后，把系统恢复到原来的状态。每次发生入侵事件，防御系统都要更新，保证相同类型的入侵事件不能再发生，所以整个 PDRR 网络安全模型包括防御、检测、响应和恢复，这四个方面组成了一个信息安全周期。

2. MPDRR 应急响应模型

MPDRR 模型是一个最常见的具有纵深防御体系的模型。MPDRR 模型包含了管理（management）、防护（protection）、检测（detection）、响应（reaction）、恢复（recovery）5 个环节。MPDRR 模型是在 PDRR 模型基础上发展而成的，它继承了 PDRR 模型的优点，并加入了 PDRR 所没有的安全管理这一环节，从而将技术和管理融为一体，整个安全体系的建立必须经过安全管理进行统一协调和实施。MPDRR 模型如图 9-3 所示。

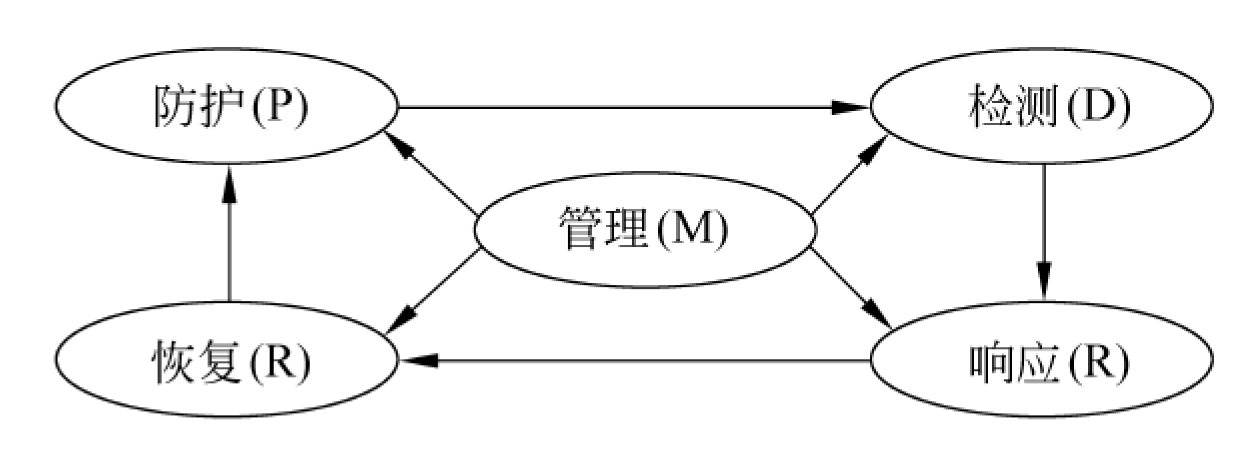


图 9-3　MPDRR 模型

9.2.2　应急响应操作流程

应急响应操作流程一般包括六个阶段，如图 9-4 所示。

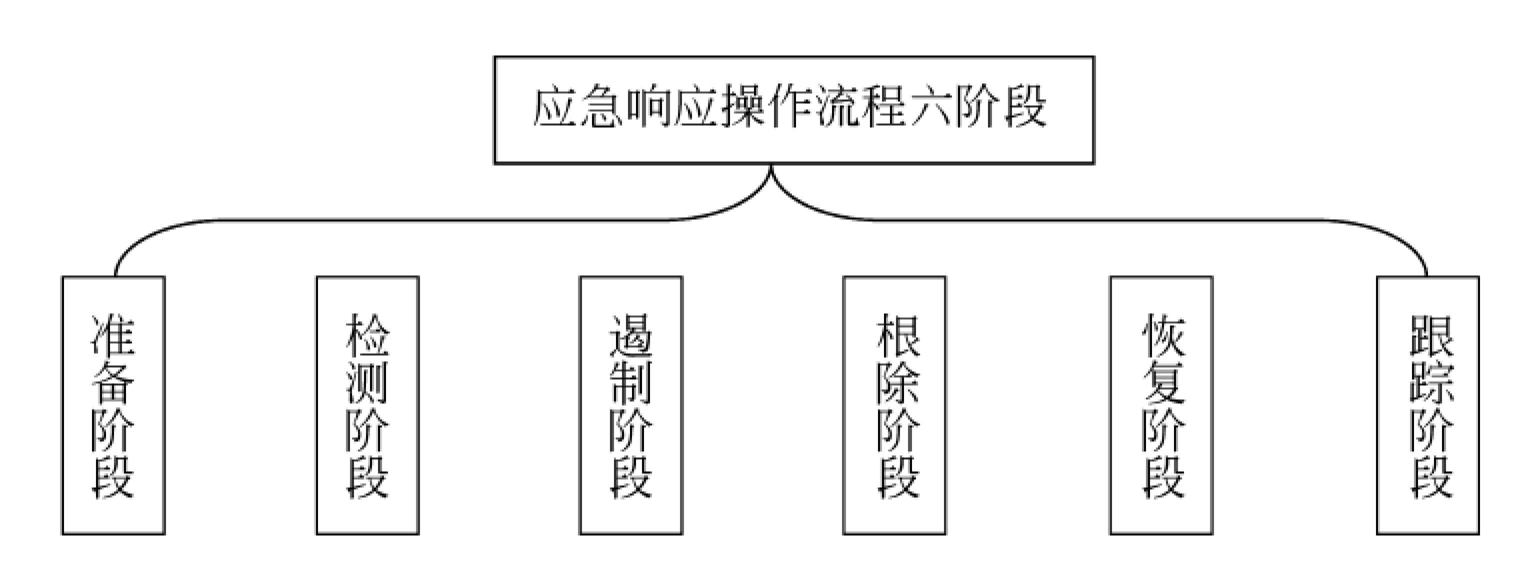


图 9-4　应急响应操作流程六阶段

1. 准备阶段：预防安全事件产生

准备阶段主要任务是预防，在事件真正发生前为应急响应做好准备。主要包括以下几项内容：

（1）制订用于应急响应工作流程的计划，并建立一组基于威胁的合理的防御/控制

措施。

（2）制订预警与报警的方法，建立一组尽可能高效的事件处理程序。

（3）建立备份的体系和流程。

（4）建立安全的系统，按照安全政策配置安全设备和软件。

（5）建立一个支持事件响应活动的基础设施，获得处理问题必需的资源和人员，进行相关的安全培训，可以进行应急响应事件处理的预演。

（6）建立数据汇总分析体系。

2. 检测阶段：确定事件性质和责任人人选

主要任务是识别和发现各种安全的紧急事件。在紧急事件发生前，产生安全的预警报告，在紧急情况发生时，产生安全警报，并报告给应急响应中心。应急响应中心根据事件的级别，采取响应的措施。主要包括以下几种处理方法：

（1）主动发现：入侵检测设备、全局预警系统。

（2）被动发现：网络使用者报告的异常情况。

（3）确定责任人人选，即指定一个责任人全权处理此事件并给予必要资源。

（4）估计事件的范围和影响的严重程度，来决定启动相应的应急响应的方案。

（5）确定事件影响了多少主机、涉及多少网络、攻击者入侵到网络内部有多远、攻击者得到了什么样的权限、风险是什么、使用了多少种攻击方法以及攻击者利用的漏洞传播的范围有多大。

（6）通过汇总，确定是否发生了全网的大规模事件。

3. 遏制阶段：及时采取行动遏制事件发展

主要任务是限制攻击的范围，同时限制潜在的损失和破坏。在第二阶段确认紧急事件发生的情况下，进入应急响应流程。应急响应系统本身将根据预先制定的规则，采取相应的措施，确保封锁方法对各网业务影响最小，协调各网一致行动，实施隔离，把紧急事件的影响降低到最小。这些措施主要包括：

（1）初步分析，重点确定适当的遏制方法，如阻断正在发起攻击的行为，缓解系统的负载，通过路由器、防火墙封堵入侵的源地址，隔离被病毒感染的系统等。

（2）修改所有防火墙和路由器的过滤规则，拒绝来自看起来是发起攻击的主机的流量。

（3）封锁或删除被攻击的登录账号。

（4）提高系统或网络行为的监控级别。

（5）设置蜜罐并关闭被利用的服务。

（6）汇总数据，估算损失和隔离效果。

4. 根除阶段：彻底解决问题隐患

主要任务是在事件被抑制以后，找出事件根源并彻底根除。此时可以采取以下措施：

（1）对于病毒，应该在信息系统内部采用最新的软件清除所有的病毒。

（2）对于系统的入侵、非法授权访问等，应查找系统到底存在哪些漏洞，从而避免类似情况的再次发生。

（3）改进安全策略。

（4）启动网络与应用层的审计功能，为进一步的分析提供详细的资料。

（5）分析事件发生的原因，为以后的进一步改善提供依据。

（6）加强宣传，公布事件的危害性和解决办法，呼吁用户解决终端问题。

5. 恢复阶段：恢复系统的正常运行

把所有受侵害或被破坏的系统、应用、数据库、网络设备等彻底地还原到它们正常的任务状态。主要的方面有：

（1）对被破坏、无法修复的数据或系统进行系统恢复，对所有安全上的变更作备份，对收到破坏的网络安全设备进行软件配置恢复。

（2）服务重新上线并持续监控，了解各网的运行情况。

（3）根据各网的运行情况判断隔离措施的有效性。

（4）通过汇总分析的结果判断仍然受影响的终端的规模。

（5）发现重要用户及时通报解决。

（6）适当的时候解除封锁措施，去掉用作短期抑制措施的所有中间防御措施。

6. 跟踪阶段：对恢复后的系统进行持续跟踪、调查

从已经发生的紧急事件出发、吸取紧急事件响应过程中的经验与教训，回顾并整合发生事件的相关信息。主要包括：

（1）关注系统恢复以后的安全状况。

（2）重点关注曾经出问题的地方。

（3）建立跟踪文档。

（4）规范跟踪记录。

（5）对响应效果给出评估。

（6）对进入司法程序的事件，进行进一步的调查，打击违法犯罪活动。

应急响应过程操作流程还可以用三阶段来描述，如图 9-5 所示。

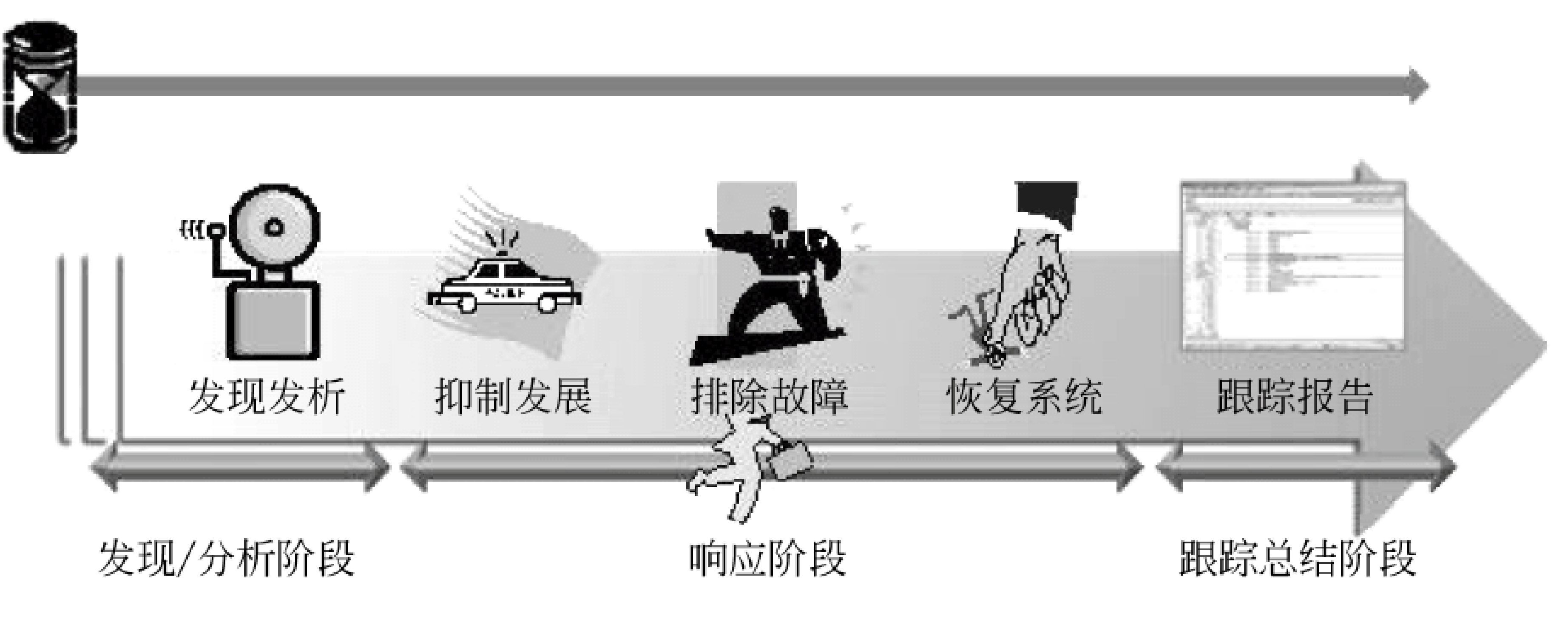


图 9-5　应急响应操作流程三阶段

9.3 数据备份

数据备份是应急响应与灾难恢复的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其他的存储介质的过程。数据备份是为了达到数据恢复和重建目标所进行的一系列备份步骤和行为。

数据备份与应急响应、灾难恢复密不可分，数据备份是应急响应、灾难恢复的前提和基础，而应急响应与灾难恢复是在此基础之上的具体应用。应急响应与灾难恢复的目标与计划决定了要采取的数据备份策略，如备份所采用的存储介质，软硬件产品都是恢复时需要考虑的因素。而应急响应与灾难恢复策略也应依据数据备份的情况来制定。

本节主要介绍数据安全问题、数据存储方式与数据备份技术。

9.3.1 数据安全问题

1. 保护数据的重要性

随着信息化建设与互联网的高速发展，各行各业的信息进入到计算机系统中，包括财务、客户信息等重要数据，计算机系统逐渐成为政府和各企事业单位的基础设施。互联网的重要性更是影响到社会生活的稳定，甚至成为敌我双方争夺的目标。而互联网中的核心资源是存储在互联网中的数据资源。

IDG公司对美国发生过信息灾难的公司进行统计，55%的公司立即倒闭，29%的公司2年后倒闭。2003年，上海发生轨道工程工地坍塌，3座大楼安全受到严重威胁。为抢救楼内的数据信息，人们冒着生命危险进入即将倒塌的楼内将存放重要数据的磁盘抢出。

计算机硬件设备毁坏后可以再购买，软件系统毁坏后可以重新安装，数据丢失了以后怎么处理？尽管灾难、战争是小概率事件，但是它们具有偶然性和突然性，不可预判，难以避免。例如四川地震、南方的雪灾、9·11事件等。因此，数据安全是需要人们高度重视的重大问题，特别是那些重要信息系统的数据安全，更是关系国家安全、经济命脉和社会稳定。

2. 数据的多样性

随着互联网的高速发展，数据也发生了巨大的变化，主要体现在：

(1) 数据存储量急剧膨胀。数据存储技术的发展和数据存储量的增长也基本符合摩尔定律，即200%/18个月。

(2) 数据访问时间和方式的全方位要求，即7*24*365随时随地提供访问。

(3) 数据结构与格式多样性。数据除了数字与文字，还可以是图形、影像、音频、视频等格式；数据结构也是多种多样。

(4) 存储设备异构性。

数据的多样性也为数据保护提出了新的技术要求。

3. 数据保护的技术与措施

如何才能保护企业与个人赖以生存和发展的数据安全？目前已经有许多数据保护的技术，最重要的是冗余技术，包括数据备份、冗余的设备、软件和人员等，还有隔离、多样性、集群技术等。

集群(cluster)技术是将一组相互独立的、通过高速网络互联的服务器构成一个组，并以单一系统的模式加以管理。一个客户与集群相互作用时，集群像是一个独立的服务器。通过集群技术，可以提高处理性能，例如一些计算密集型应用天气预报、核试验模拟等；可以降低成本，在达到同样性能的条件下，采用集群比采用同等运算能力的大型服务器具有更高的性价比；将新的服务器加入集群可以提高可扩展性；最重要的是可以增强可靠性，集群技术使系统在故障发生时仍可以继续工作，当一个应用服务发生故障时，应用服务将被重新启动或被另一台服务器接管，使系统停运时间减到最小。集群系统在提高系统的可靠性的同时，也大大减小了故障损失。

除了采用技术手段，还需要制定数据安全规划与制度。

9.3.2 数据存储技术

数据存储是数据备份的技术基础，技术产品主要有磁盘与磁盘阵列、磁带机(最为成熟、性价比好)与磁带库、光盘与光盘库等。存储方式主要有直接附加存储、网络附加存储、区域网络存储、分级存储、虚拟存储等。

1. 存储介质

(1) 磁盘与磁盘阵列。

磁盘包括软盘、硬盘、U 盘、移动硬盘等，是最常见的存储设备。

磁盘阵列(redundant arrays of inexpensive disks，RAID)是利用数组方式来作磁盘组，配合数据分散排列的设计，提升数据的安全性。磁盘阵列是由很多便宜、容量较小、稳定性较高、速度较慢磁盘，组合成一个大型的磁盘组，利用个别磁盘提供数据所产生的集成效果提升整个磁盘系统效能。磁盘阵列将数据切割成许多区段，分别存放在各个硬盘上。它能利用同位检查(parity check)的观念，在数组中任一个硬盘发生故障时，仍可读出数据，在数据重构时，将数据经计算后重新置入新硬盘中。它特别适用于既有大量数据需要存取，同时又对数据安全性要求严格的领域，如银行、金融、商业超市、仓储库房、各种档案管理等。

(2) 磁带机与磁带库。

磁带是单位存储信息成本最低、容量最大、标准化程度最高的常用存储介质之一。它互换性好、易于保存，近年来由于采用了具有高纠错能力的编码技术和即写即读的通道技术，大大提高了磁带存储的可靠性和读写速度。缺点是读写速度慢。

磁带机(tape drive)一般指单驱动器产品，通常由磁带驱动器和磁带构成，是一种经济、可靠、容量大、速度快的备份设备。

磁带库一般包括自动加载磁带机和磁带库。自动加载磁带机和磁带库实际上是将磁

带和磁带机有机结合组成的。自动加载磁带机是一个位于单机中的磁带驱动器和自动磁带更换装置,它可以从装有多盘磁带的磁带匣中拾取磁带并放入驱动器中,或执行相反的过程。它可以备份 100GB～200GB 或者更多的数据。自动加载磁带机能够支持例行备份过程,自动为每日的备份工作装载新的磁带。

(3) 光盘与光盘库。

光盘的全称是高密度光盘(compact disc),是近代发展起来不同于磁性载体的光学存储介质,用聚焦的氢离子激光束处理记录介质的方法存储和再生信息,又称激光光盘。它信息存储容量大、记录速度快、信息不易丢失、便于长期保存、便于拷贝复制。

光盘库是一种带有自动换盘机构(机械手)的光盘网络共享设备。光盘库一般由放置光盘的光盘架、自动换盘机构(机械手)和驱动器三部分组成。光盘库一般配置有 1～12 台 CD-ROM 驱动器,可容纳 50～600 片 CD-ROM 光盘。

光盘塔是由很多光驱连接在一起的一种设备,可以同时在多个光盘上读写数据,就像磁盘阵列一样。

光盘镜像服务器是一种网络附加存储设备,它采用硬盘高速缓存技术,将整张光盘的内容存储(镜像)到硬盘中。这样,用户就可以以硬盘的速度来共享服务器中的镜像光盘。

2. 存储方式

(1) DAS(direct attached storage)——直接附加存储。

DAS 存储相对比较传统,采用这种 DAS 技术的存储服务器,其物理结构跟 PC 类似。把外部磁盘阵列、磁带机等设备直接连到服务器总线上,外部存储设备相当于服务器整机的一部分。

(2) NAS(network attached storage)——网络附加存储。

NAS 用一个文件服务器连接所有存储设备自形成一个网络存储系统,其不再通过 I/O 总线附属于某个特定的服务器或客户机,而是直接通过网络接口与网络直接相连,这样数据存储就不再是服务器的附属,而是作为独立网络节点而存在于网络之中,可由所有的网络用户共享。

(3) SAN(storage area network)——区域网络存储。

SAN 是一种通过光纤集线器、光纤路由器、光纤交换机等连接设备将磁盘阵列、磁带等存储设备与相关服务器连接起来的高速专用子网,它用光纤保障存储设备之间、存储设备与企业网络之间的快速连通,同时具有扩展性能。

(4) 分级存储。

根据数据的活跃程度,分别存储在不同的设备上。如活跃数据(在线存储)、近期历史数据(近线存储)以及存档数据(离线存储)。

(5) 虚拟存储。

虚拟存储技术将底层存储设备进行抽象化统一治理,向服务器层屏蔽存储设备硬件的差异(异构性),提供统一的逻辑特性,从而实现了存储系统集中、统一而又方便的治理。

9.3.3 数据备份技术

1. 数据备份的定义与意义

(1) 定义。

数据备份就是将数据加以保存,以便在系统遭受破坏或其他特定情况下,重新加以利用进行系统恢复的一个过程。

(2) 意义。

数据备份与数据恢复是保护数据的最后手段,也是防止信息攻击的最后一道防线。数据备份的根本目的是重新利用,备份工作的核心是恢复。一个无法恢复的备份,对任何系统来说都是毫无意义的。

另外,数据备份的意义不仅在于防范意外事件的破坏,而且还是历史数据保存归档的最佳方式。

(3) 与容灾或集群技术的区别。

集群和容灾技术的目的是为了保证系统的可用性。对数据而言,集群和容灾技术保护系统的在线状态,保证当意外发生时数据可以被随时访问,系统所提供的服务和功能不会因此而间断。

而备份技术的目的是将整个系统的数据或状态保存下来,通常采用离线保存的方式(与当前系统隔离开)。一般来说,备份技术并不保证系统的实时可用性。在恢复过程中,系统是不可用的。

因此,在运行关键任务的系统中,备份技术、集群技术和容灾技术互相不可替代。

2. 构建数据备份原则

(1) 可靠性,是指自身工作要稳定可靠。

(2) 全面性,是指能支持各种操作系统、不同的数据库和典型应用。

(3) 自动化,是指具有自动备份、自动更换磁带、自动报警的功能。

(4) 高性能,是指可以尽量提高数据传送速度,在休息时间完成数据备份。

(5) 不干扰应用系统的运行,是指一些关键系统要求 24 小时运行,备份工作应不间断系统的运行,且尽量不影响系统的工作性能。

(6) 容灾考虑,根据自身业务需要,可以考虑是否建立异地容灾备份系统。

(7) 数据的最终归宿问题,数据销毁与归档机制。

3. 数据备份分类

(1) 依据备份的数据量分类。

① 全备份:即备份系统中的所有数据,备份时间周期分为大小两类,一般为周和天。优点:恢复时间短,最可靠,操作方便;缺点:数据量大,备份时间长,空间消耗大。

② 增量备份:即备份上一次备份以后更新的所有数据。优点:备份时间短,空间消耗小;缺点:恢复操作复杂,需要一个全备份,以及其后的所有增量备份。

③ 差分备份：即备份上一次全备份以后更新的所有数据。恢复相对简单，只需上一次全备份以及最近一次差分备份。优缺点介于上两者之间。

④ 综合型完全备份：是指通过完全备份、差分备份和增量备份的信息创建一个新的完全备份（离线），综合型完全备份一般是在当备份时间较短时进行。

（2）依据备份形式分类。

① 物理备份：是指将实际物理数据库文件从一处复制到另一处的备份，冷备份、热备份都属于物理备份。

② 逻辑备份：是指将某个数据库的记录读出并将其写入到一个文件中，这是经常使用的一种备份方式。

（3）依据备份时间分类。

① 冷备份（脱机备份）：是指以正常方式关闭数据库，并对数据库的所有文件进行备份。缺点是中断应用系统相关服务，不易做到实时备份。

② 热备份（联机备份）：是指在数据库打开和用户对数据库进行操作的情况下进行的备份，例如：通过使用数据库系统的复制服务器，连接正在运行的主数据库服务器和热备份服务器，当主数据库的数据修改时，变化的数据通过复制服务器可以传递到备份数据库服务器中，保证两个服务器中的数据一致。热备份方式是一种实时备份。

（4）依据备份实现的层次分类。

① 硬件冗余：硬件冗余技术有双机容错、磁盘双工、磁盘阵列（RAID）与磁盘镜像等多种形式。硬件冗余技术使系统据有充分的容错能力，对于提高系统的可靠性非常有效，硬件冗余的不足在于：不能解决因病毒或人为误操作引起的数据丢失以及系统瘫痪等灾难，如果错误数据也写入备份磁盘，硬件冗余也会无能为力。

② 软件备份：利用各种软件措施实施数据和系统备份，理想的备份系统应是硬件容错加软件备份。

（5）依据备份地点分类

① 本地备份：备份的数据、文件存放在本地，其缺点是不能防范地震、火灾等重大灾害。

② 异地备份：备份的数据、文件异地存放，因而具有更高的安全性，但成本较高。

4. 制定数据备份策略的规则

数据备份的策略是指确定需要备份的内容、备份时间以及备份方式。常用的备份策略有完全备份、增量备份、差分备份以及这三种备份策略的组合。制定备份策略时可以参考如下规则：

（1）对于操作系统和应用程序代码，可在每次系统更新或安装新软件时做一次全备份。

（2）对于日常更新量很大，但总体数据量不是很大的关键应用数据库，可在每天用户使用量较小的时段安排做全备份。

（3）对于总体数据量很大，但日常更新量相对较小的关键应用数据库，可每隔一周或更长时间做一次全备份，而每隔一个较短的时间（如：每天）做一次增量备份。

5. 数据备份的方式

简单来说，数据备份主要有 LAN 备份、LAN Free 备份和 SAN Server-Free 备份三种。LAN 备份针对所有存储类型都可以使用，LAN Free 备份和 SAN Server-Free 备份只能针对 SAN 架构的存储。

(1) LAN 备份。

传统备份需要在每台主机上安装磁带机备份本机系统，采用 LAN 备份策略，在数据量不是很大的时候，可采用集中备份。一台中央备份服务器将会安装在 LAN 中，然后将应用服务器和工作站配置为备份服务器的客户端。中央备份服务器接受运行在客户机上的备份代理程序的请求，将数据通过 LAN 传递到它所管理的、与其连接的本地磁带机资源上。这一方式提供了一种集中的、易于管理的备份方案，并通过在网络中共享磁带机资源提高了效率。

(2) LAN-Free 备份。

LAN-Free 备份主要指快速随机存储设备(磁盘阵列或服务器硬盘)向备份存储设备(磁带库或磁带机)复制数据，备份服务器通过 SAN 连接到磁带机上，在 LAN-Free 备份客户端软件的触发下，读取需要备份的数据，通过 SAN 备份到共享的磁带机。这种独立网络不仅可以使 LAN 流量得以转移，而且它的运转所需的 CPU 资源低于 LAN 方式，这是因为光纤通道连接不需要经过服务器的 TCP/IP 栈，而且某些层的错误检查可以由光纤通道内部的硬件完成。在许多解决方案中需要一台主机来管理共享的存储设备以及用于查找和恢复数据的备份数据库。LAN-Free 备份架构如图 9-6 所示。

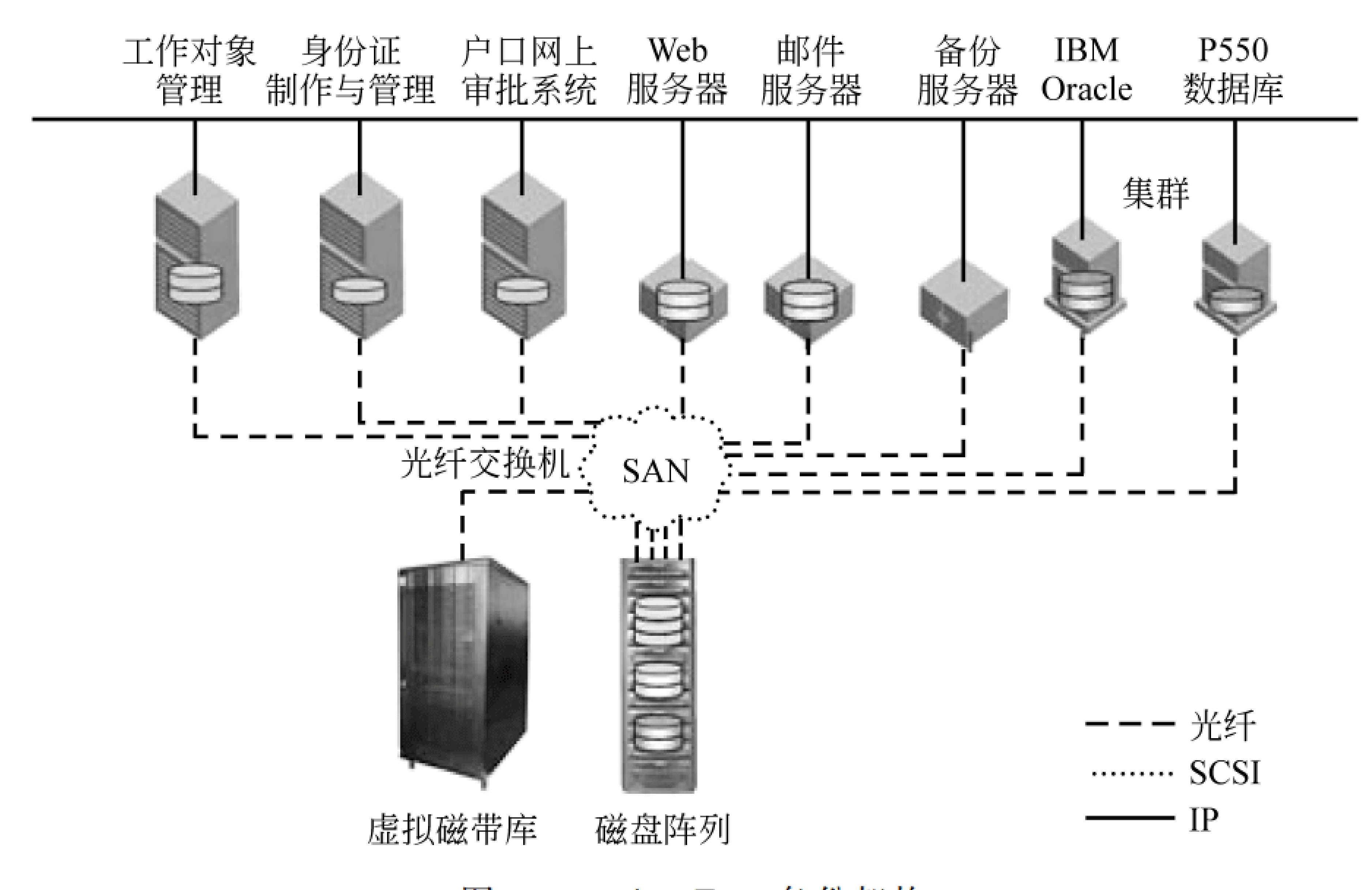


图 9-6 LAN-Free 备份架构

(3) SAN Server-Free 备份。

LAN Free 备份需要占用备份主机的 CPU 资源，SAN Server-Free 备份既不占用网络带宽，也不占用服务器额外时间，备份过程能够在 SAN 内部完成，大量数据流无须流

过服务器，可以极大地降低备份操作对系统的影响。SAN Server-Free 备份架构如图 9-7 所示。

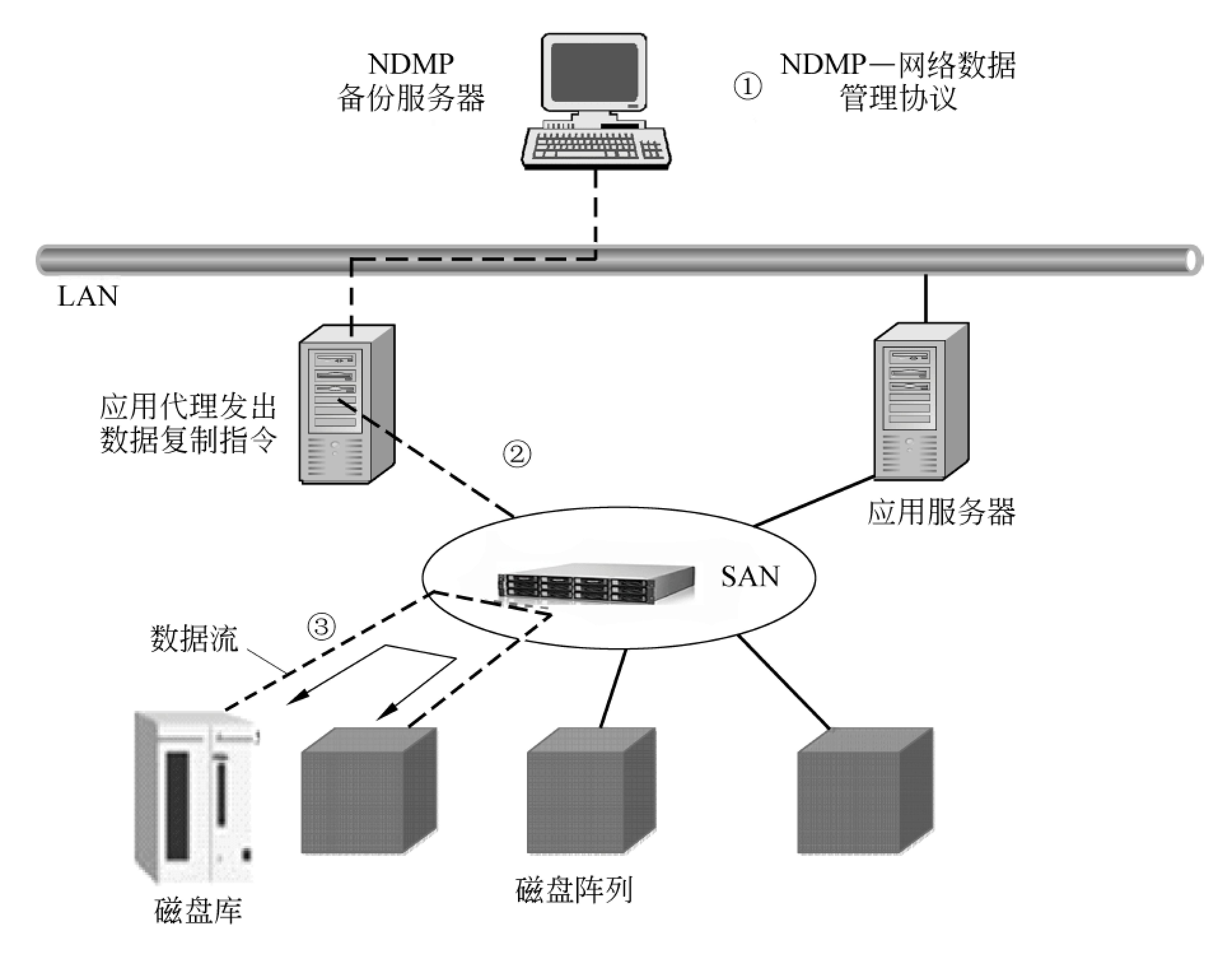


图 9-7　SAN Server-Free 备份架构

9.4　灾难恢复与容灾建设

灾难恢复的目的是在灾难发生后尽快地恢复系统运行，减少因系统被破坏而造成的业务停顿时间，使灾难造成的损失降低到最低。容灾是指对灾难的容忍，是为了保证关键业务和应用在经历各种灾难后，仍然能够最大限度地提供正常服务所进行的一系列计划及建设行为。

本节主要介绍灾难恢复指标与等级、灾难恢复需求分析、灾难恢复资源与策略以及容灾建设与计划。

9.4.1　灾难恢复指标与等级

衡量灾难恢复经常使用以下两个指标：

1. 恢复点目标——RPO

RPO(recovery point objective)灾难发生后，系统和数据必须恢复到的时间点要求，用来描述企业可以容忍的最大数据丢失量。如果数据备份周期是 1 天，那么最大数据丢失量就是最近 24 小时的数据。

2. 恢复时间目标——RTO

RTO(recovery time objective)是灾难发生后,信息系统或业务功能从停顿到恢复使用的时间要求。即所能容忍的业务中断的最长时间。采用应用级异地容灾技术,可将RTO缩短到几分钟;而采用传统的磁带备份,可能需要数日,甚至数月的时间。

RPO针对的是数据丢失,而RTO针对的是服务丢失,二者没有必然的关联性。RTO和RPO的确定必须在进行风险分析和业务影响分析后根据不同的业务需求确定。对于不同企业的同一种业务,RTO和RPO的需求也会有所不同。RPO和RTO越小,系统的可用性就越高,当然用户需要的投资也越大。

3. 灾难恢复等级

根据2005年4月国务院信息化工作办公室《重要信息系统灾难恢复指南》的要求,灾难恢复等级分为6级:

等级1:基本支持。要求数据备份系统能够保证每周至少进行一次数据备份,备份介质能够提供场外存放。对于备用数据处理系统和备用网络系统,没有具体要求。

等级2:备用场地支持。在满足等级1的条件基础上,要求配备灾难恢复所需的部分数据处理设备,或灾难发生后能在预定时间内调配所需的数据处理设备到备用场地;要求配备部分通信线路和相应的网络设备,或灾难发生后能在预定时间内调配所需的通信线路和网络设备到备用场地。

等级3:电子传输和设备支持。要求每天至少进行一次完全数据备份,备份介质场外存放,同时每天多次利用通信网络将关键数据定时批量传送至备用场地。配备灾难恢复所需的部分数据处理设备、通信线路和相应的网络设备。

等级4:电子传输及完整设备支持。在等级3的基础上,要求配置灾难恢复所需的所有数据处理设备、通行线路和相应的网络设备,并且处于就绪或运行状态。

等级5:实时数据传输及完整设备支持。除要求每天至少进行一次完全数据备份,备份介质场外存放外,还要求采用远程数据复制技术,利用通信网络将关键数据实时复制到备用场地。

等级6:数据零丢失和远程集群支持。要求实现远程实时备份,数据零丢失;备用数据处理系统具备与生产数据处理系统一致的处理能力,应用软件是“集群的”,可实时无缝切换。

由此可见,灾难恢复能力等级越高,对于信息系统的保护效果越好,但同时成本也会急剧上升。因此,需要根据成本风险平衡原则(即灾难恢复资源的成本与风险可能造成的损失之间取得平衡),确定业务系统的合理的灾难恢复能力等级。对于多个业务系统,不同业务可采用不同的灾难恢复策略。

9.4.2 灾难恢复需求分析

灾难恢复需求分析包括风险分析和业务影响分析。

1. 风险分析

风险分析主要包括标识信息系统的资产价值、识别信息系统面临的自然和人为威胁、识别信息系统的脆弱性、分析各种威胁发生的可能性,并定量或定性描述可能造成的损失。依据防范或控制风险的可行性和残余风险的可接受程度,确定对风险的防范和控制措施,确定防范或控制信息系统风险的技术或管理手段。

2. 业务影响分析

(1) 分析业务功能和相关资源配置。

分析单位的各项业务功能及各项业务之间的相关性,确定支持各种业务功能的相应信息系统资源及其他资源,明确相关信息的保密性、完整性和可用性要求。

(2) 评估中断影响。

应采用定量和/或定性的方法,对各种业务功能的中断造成的影响进行评估。

(1) 定量分析:以量化方法,评估业务功能的中断可能给单位带来的直接经济损失和间接经济损失;

(2) 定性分析:以非量化方法,评估业务功能的中断可能对国家的政治、社会、法律及单位内部事务等造成的影响。

3. 确定灾难恢复目标

根据风险分析和业务影响分析的结果,确定灾难恢复目标,包括:

(1) 关键业务功能及恢复的优先顺序;

(2) 灾难恢复时间范围,即 RTO 和 RPO 的范围。

9.4.3 灾难恢复资源与策略

灾难恢复资源包括数据备份系统、备用基础设施、备用数据处理系统、备用网络系统、技术支持能力、运行维护管理能力和灾难恢复预案。

灾难恢复策略包括灾难恢复资源的获取方式与灾难恢复等级各要素的具体要求。

1. 数据备份系统

数据备份系统一般由数据备份的硬件、软件和数据备份介质(以下简称“介质”)组成,如果是依靠电子传输的数据备份系统,还包括数据备份线路和相应的通信设备。

数据备份系统可由单位自行建设,也可通过租用其他机构的系统而获取。

企业应根据灾难恢复目标,按照成本风险平衡原则,确定:数据备份的范围;数据备份的时间间隔;数据备份的技术及介质;数据备份线路的速率及相关通信设备的规格和要求。

2. 备用基础设施

备用基础设施是灾难恢复所需的、支持灾难备份系统运行的建筑、设备和组织,包括

介质的场外存放场所、备用的机房及工作辅助设施，以及容许灾难恢复人员连续停留的生活设施。

可采用以下三种方式获取备用基础设施：

（1）由单位所有或运行；

（2）由多方共建或通过互惠协议获取；

（3）租用商业化灾难备份中心的基础设施。

对备用基础设施的要求，包括：与生产系统所在的数据处理中心（以下简称“生产中心”）的距离要求；场地和环境（如面积、温度、湿度、防火、电力和工作时间等）要求；运行和管理要求。

3．备用数据处理系统

可选用以下三种方式之一来获取备用数据处理系统：

（1）事先与厂商签订紧急供货协议；

（2）事先购买所需的数据处理设备并存放在灾难备份中心或安全的设备仓库；

（3）利用商业化灾难备份中心或签有互惠协议的机构已有的兼容设备。

企业应根据关键业务功能的灾难恢复对备用数据处理系统的要求和未来发展的需要，确定备用数据处理系统的数据处理能力、与生产系统的兼容性要求、平时处于就绪还是运行状态。

4．备用网络系统

备用网络系统包含备用网络通信设备和备用数据通信线路，备用网络通信设备与获取备用数据处理系统方式相同；备用数据通信线路可使用自有数据通信线路或租用公用数据通信线路。

企业应根据关键业务功能的灾难恢复对网络容量及切换时间的要求和未来发展的需要，选择备用数据通信的技术和线路带宽，确定网络通信设备的功能和容量，保证灾难恢复时，最终用户能以一定速率连接到备用数据处理系统。

5．技术支持能力

可选用以下几种方式获取技术支持能力：

（1）灾难备份中心设置专职技术支持人员；

（2）与厂商签订技术支持或服务合同；

（3）由生产系统技术支持人员兼任；但对于 RTO 较短的关键业务功能，应考虑到灾难发生时交通和通信的不正常，造成技术支持人员无法提供有效支持的情况。

企业应根据灾难恢复目标，确定灾难备份中心在软件、硬件和网络等方面的技术支持要求，包括技术支持的组织架构、各类技术支持人员的数量和素质等要求。

6．运行维护管理能力

可选用以下对灾难备份中心的运行维护管理模式：

(1) 自行运行和维护;
(2) 委托其他机构运行和维护。
企业应根据灾难恢复目标,确定灾难备份中心运行维护管理要求,包括运行维护管理组织架构、人员的数量和素质、运行维护管理制度等要求。

7. 灾难恢复预案

可采用以下方式,完成灾难恢复预案的制订、落实和管理:
(1) 由单位独立完成;
(2) 聘请外部专家指导完成;
(3) 委托外部机构完成。
企业应根据灾难恢复需求分析的结果,明确灾难恢复预案的整体要求、制订过程的要求、教育、培训和演练要求以及管理要求。

9.4.4 容灾建设与计划

数据安全关乎国计民生,银行、电力、铁路、民航、证券、保险、海关、税务等行业和电子政务部门必须进行容灾建设。

1. 灾难建设的基本原则

(1) 统筹规划,合理布局。
(2) 资源共享,互为备份。
(3) 分级管理,合理选择方案,避免"过保护"和"欠保护"。
(4) 不要忽视"日常灾害",只片面强调"大灾难"。
(5) 平灾结合,灾难恢复是为小概率事件服务的,平常可能是闲置状态。在不影响其容灾功能的前提下,加强这些设备在平时的使用效率,物尽其用。

2. 容灾建设类型

(1) 按照容灾所保障的内容可以分为数据容灾和应用容灾。
① 数据容灾通过在异地建立一份数据复制的方式保证数据的完整性、可靠性和安全性,当本地工作系统出现不可恢复的物理故障时,容灾系统提供可用的数据。数据级容灾是容灾的基础形式,由于只需要考虑数据的复制和存放,不需要考虑备用系统,实现起来相对简单,投资也较少。但系统提供的实时服务在灾难发生时可能会中断,用户的应用服务请求不能得到及时响应。
② 应用容灾则是在数据容灾之上,建立一套与生产系统相当的备份应用系统。在灾难发生后,将应用迅速切换到备用系统,备份系统承担生产系统的业务运行。
(2) 按照容灾功能实现的距离远近可以分为本地容灾与异地容灾。
本地容灾:即将系统数据或应用在本地备份,无异地后援。一般在相近区域建立两个数据中心:一个为生产中心,负责日常生产运行;一个为灾难备份中心。本地容灾由于距离近,带宽大,经常采用同步镜像。这一级别的容灾,仅能应付本地的硬件损坏、人为因

素造成的灾难、火灾，建筑物倒塌等灾害。

异地容灾：生产中心与灾难备份中心至少相距100km以上，可以采用同步镜像，能防范地震、水灾和战争等。异地容灾还可以细分为：

① 异地数据冷备份（冷站）：即将系统数据备份到物理介质（磁盘、磁带或光盘）上，然后送到异地进行保存。这种方案成本低、易于实现。但是在灾难发生时，数据的丢失量大，并且系统需要很长的恢复时间，无法保持业务的连续性。

② 异地数据热备份（热站）：即在异地建立一个热备份中心，采取同步或者异步方式，通过网络将生产系统的数据备份到备份系统中。备份系统只备份数据，不承担生产系统的业务。当灾难发生时，数据丢失量小，甚至零丢失，但是，系统恢复速度慢，无法保持业务的连续性。

③ 异地应用级容灾：即在异地建立一个与生产系统相同的备用系统，备用系统与生产系统共同工作，承担系统的业务。这种容灾系统，能够提供很小的数据丢失量，系统恢复速度最快。但需要配置复杂的系统管理软件和专用的硬件，相对成本也是最高的。

3. 容灾中心建设方式

（1）自行建设。

（2）委外托管，为减少容灾中心建设的高额成本，可以利用第三方的服务——将容灾中心托管给专门机构。

（3）合作备份（reciprocal site）：通过合同或契约的形式与友好的企业共享服务器与备份数据，这个方案可以节省大量的费用，但同时带来了大量的安全隐患。

4. 容灾计划

自“9·11事件”之后，全球各企业均认识到灾难防范保护的重要性。华尔街的金融机构重新对灾难恢复的步骤做了评估，并认识到灾难恢复只是技术手段之一，它们开始强调业务连续性（business continuity）而不仅仅是灾难恢复（disaster recovery）。因为过去的“灾难”恢复计划并没有强调全局性及对整个市场的影响，而如何维持业务的连续运作将成为企业运营风险评估中至关重要的一环。事实证明，只有对数据存储备份制定完备、持续且可执行的容灾计划，特别是业务连续计划，才能为人们提供万无一失的数据安全保护。

容灾计划应包括一系列应急计划，如业务持续计划，业务恢复计划，操作连续性计划，应急响应计划，场所紧急计划，危机通信计划，灾难恢复计划等。

（1）业务持续计划（business continuity plan，BCP）。

它是一套用来降低组织的重要营运功能遭受未料的中断风险的作业程序，它可能是人工的或系统自动的。业务持续计划是高层管理人员的首要职责，因为他们被委任于保护公司的资产及公司的生存。业务持续计划的目的是使得一个组织及其信息系统在灾难事件发生时仍可以继续运作。为了能对灾难事件有适当的对策，严密的计划及相关资源的投入是必需的。

（2）业务恢复计划（business recovery plan，BRP）。

它也叫业务继续计划，涉及紧急事件后对业务处理的恢复，但与BCP不同，它在整个

紧急事件或中断过程中缺乏确保关键处理的连续性的规程。BRP 的制定应该与灾难恢复计划及 BCP 进行协调。BRP 应该附加在 BCP 之后。

(3) 操作连续性计划(continuity of operations plan,COOP)。

COOP 关注位于机构(通常是总部单位)备用站点的关键功能以及这些功能在恢复到正常操作状态之前最多 30 天的运行。由于 COOP 涉及总部级的问题,它和 BCP 是互相独立制定和执行的。COOP 的标准要素包括职权条款、连续性的顺序和关键记录和数据库,主要强调机构在备用站点恢复运行中的能力。

(4) 应急响应计划(incident response plan,IRP)。

应急响应计划建立了处理针对机构的 IT 系统攻击的规程。这些规程用来协助安全人员对有害的计算机安全事件进行识别、消减并进行恢复。

(5) 场所紧急计划(occupant emergency plan,OEP)。

OEP 在可能对人员的安全健康、环境或财产构成威胁的事件发生时,为设施中的人员提供反应规程。OEP 在设施级别进行制定,与特定的地理位置和建筑结构有关。设施 OEP 可以附加在 BCP 之后,但是独立执行。

(6) 危机通信计划(crisis communication plan,CCP)。

机构应该在灾难之前做好其内部和外部通信规程的准备工作。危机通信计划通常由负 责公共联络的机构制定。危机通信计划规程应该和所有其他计划协调,以确保只有受到批准的内容公之于众,它应该作为附录包含在 BCP 中。通信计划通常指定特定的人员作为在灾难反应中回答公众问题的唯一发言人。它还可以包括向个人和公众散发状态报告的规程,例如记者招待会的模板。

(7) 灾难恢复计划(disaster recovery plan,DRP)。

正如其名字所表示的,DRP 应用于重大的、通常是灾难性的、造成长时间无法对正常设施进行访问的事件。通常,DRP 指用于紧急事件后在备用站点恢复目标系统、应用或计算机设施运行的 IT 计划。DRP 的范围可能与应急响应计划重叠,但是 DRP 的范围比较狭窄,它不涉及无须重新配置的小型危害。根据机构的需要,可能会有多个 DRP 附加在 BCP 之后。

9.5 容错系统

由于网络攻击与系统故障无法完全避免,为了使信息系统能够容忍系统故障或入侵的发生,并能正常工作,人们提出了容错系统与自恢复系统,容错系统与自恢复系统在受到入侵攻击与灾难事件后的不正确行为,当作一种系统故障,利用容错技术,来保证系统的正确执行,容错系统与自恢复系统是计算机安全技术研究的新课题。

本节主要介绍容错系统与自恢复系统的关键技术容错技术,它为计算机系统提供了这样的能力:当计算机内部出现故障时,计算机系统仍能正确工作,下面简要介绍容错系统中使用的其他技术与容错系统工作过程。

9.5.1 容错系统与容错计算机

1. 容错系统

系统的故障可分为两类：一类是“致命的”，不可能自行修复，例如系统的主要部件全部损坏；另一类是局部的，可能被修复，例如部分元件失效、线路故障、偶然干扰引起的差错等。

容错系统就是利用容错技术构造的一种能够自动排除非致命性故障的系统。容错系统不是凭空想象的，人就是一种高度完善的容错系统，人脑由 1 万亿个脑细胞构成，据估计脑细胞每天要死亡约 10 万个，但人脑却能正常工作。

容错系统采用特别的硬件、软件和电源部件，能够支持系统的备份和避免系统故障以维持系统的运行。系统装有特殊的存储芯片、处理器和磁盘存储设备，利用诸如扩充的程序流监控机制等特殊的软件程序或自我检查逻辑来检测故障以及自动转换到备份上继续工作。该机制使得系统既能容忍故意逻辑故障又能容忍随机物理故障。系统上的零部件可以移动和修理而不破坏计算机系统。

容错系统具有对故障的容许能力和自测试能力，包括硬件容错与软件容错两部分。硬件容错是指电子计算机在工作过程中，一旦硬件部分发生故障，在容错功能电路的支持下，自动进行切换，用正常的电路部分代替故障电路部分，从而保证系统不间断地连续运行，保证原定计算方法或运行程序准确地执行及完成的能力。软件容错是指对软件错误的容许程度以及支持硬件容错的相应软件功能。

2. 容错计算机

无论采用硬件方式，还是采用软件方式使之具有故障自检能力，并保证继续正确运行的电子计算机系统即称为容错计算机。容错计算机一般要达到以下目标：

(1) 高可靠性——系统出现偶发性永久性故障时仍能连续正确地运行。

(2) 不间断运行——系统发生永久性故障后仍能正常运行，并不降低效率。

(3) 实时操作——系统发生故障后能以最短时间检测、隔离故障部件，并自动恢复。

(4) 采用通用部件——采用通用部件的目的是使用现有软件向容错计算机系统进行升级。

(5) 软件透明性——容错功能的实现并不使用户感到正在使用容错计算机，而如同使用其他一般电子计算机一样。

(6) 动态可靠性选择——动态降低可靠性而提高整体性能的选择。

容错计算机一般属于小型机或中型机范畴，其配套软件较为丰富。例如，可配置虚拟操作系统，多种数据库，支持多种高级语言，并具有很强的调试功能及管理功能。

9.5.2 容错技术

容错技术是保证系统在某些组成部分出现故障或差错时仍能正常工作的技术。

1. 容错系统理论的基础

20 世纪 50 年代中期，冯·诺依曼提出容错技术中的复合冗余方法。他应用概率论证明了，可以用不甚可靠的器件堆成一个可靠的具有相同功能的组件。同期又出现了莫尔-香农冗余方法。这些研究奠定了容错系统理论的基础。

复合冗余方法构成的复合线路就是由包含多个谢弗门（输入端带有反相器的或门）的随机重复线路的串联。这种方法是对可靠性的计算基于元件出错概率服从高斯分布的假定。莫尔-香农冗余方法是用另一种方式组合继电器，用组合概率的方法分析可靠性。

两种方法都可以构成同样可靠的线路。当对系统可靠性要求并不十分高而元件可靠性又比较高时，莫尔-香农方法所用元件数比复合冗余方法少很多。当要求系统可靠性很高时，复合冗余方法又较优越。

2. 自检技术

自检技术指系统在发生非致命性故障时能自动发现故障和确定故障的性质、部位，并自动采取措施更换和隔离产生故障的部件。自检需采用诊断技术，常用专门程序实现，属于程序设计的范围。容错系统的实现要求系统必须具有重复部件或备份部件，或具有不止一个完成某种功能的通道。因此自检技术常配合冗余技术使用。

3. 冗余技术

容错技术是建立在冗余技术基础之上的。冗余技术又称储备技术，它是利用系统的并联模型来提高系统可靠性的一种手段。

根据资源的不同，冗余技术分为硬件冗余、软件冗余、时间冗余和信息冗余。

（1）硬件冗余。

硬件冗余是通过外加硬件的方式来达到系统容错目的的容错方式，该技术广为采用。它是用两倍、四倍甚至更多的元件堆积重复，相互并联，从而增加系统的可靠性。硬件冗余的部件可以是并行工作的，也可以只有一个模块工作，而其他模块则处于待命状态。一旦工作模块出现故障，立即切换到备份的模块之一。这种系统必须具备检错和切换能力。

（2）软件冗余。

软件容错技术是指开发容错软件的适宜环境和系统方法，其主要目的是提供足够的冗余信息与算法程序，使系统在实际运行过程中能够及时发现程序错误，采取补救措施，保证整个计算的正确运行。

软件容错的主要任务是研究如何将具有设计差异、对应同一任务采用的不同软件程序组成一个有机的整体，完成错误检测、程序系统重组及系统恢复等多项功能，达到利用设计差异实现容错的目的。

（3）时间冗余。

时间冗余是指以重复执行指令（指令复执）或程序（程序复算）来消除瞬时错误带来的影响。其典型应用是程序卷回。这种技术用来检验一段程序完成时的计算数据，如发现有错，则卷回继续重算那一部分。如果一次卷回不解决问题，还可多次卷回，直到故障消

除或判定不能消除故障为止。

（4）信息冗余。

信息冗余是靠增加信息的多余度来提高可靠性的，这些附加的信息位具有如下功能：当代码中某些信息位发生错误（包括附加位本身的错误）时能及时发现错误检错，或者能恢复原来的信息纠错。在数字系统中的信息传送和算术逻辑运算中广泛使用的奇偶码、海明码、乘积码、循环码，以及各种算术误差码都有很强的检错或纠错能力。

信息冗余的优点是增加的冗余度较其他方法低，而且许多码的信息位和校验位在运算中可统一处理。此外，还便于处理瞬时错误，提供故障的自检测、自定位和自纠错能力。缺点是产生时延，难于纠正编码器和译码器本身的错误。

根据冗余技术中线路的物理连接方式可以分为重复线路和备份线路。

（1）重复线路指用多个相同品种和规格的元件或组件并联起来，当作一个元件或组件使用，只要有一个不出故障系统就能够正常工作。在并联工作时每一个组件的可靠性概率是互相独立的。

（2）备份线路与重复线路的区别是参加备份的组件不接入系统，只在处于工作状态的组件发生故障时才把输入和输出接到备份组件上，同时切断故障组件的输入输出。系统具有自动发现故障的能力和自动转接的设备。若系统的某一组件发生故障使系统出现错误输出，该输出又使重复线路的共同输出产生错误，则并联方式反而降低可靠性。此时可采用备份线路或采用其他规则，例如复合冗余方法和莫尔-香农冗余方法，把组件组合起来，仍能有效地提高系统可靠性。

冗余技术提高可靠性的代价是增加了硬件费用。特别是复合冗余方法需要复合成千上万次，例如针对人脑神经系统的计算表明需要用 66 000 个细胞复合代替一个细胞，才能保证不发生误差的间隔为 10 000 年。随着大规模集成电路的发展，这种设计思想的实际应用已逐步成为可能。而大量采用重复电路和备份电路则早已成为提高可靠性的切实可行的有效方法。对于一定数量的备份元件，使系统可靠性最高的元件组合方式称为最优冗余结构。例如，当元件失效率与所受负荷成正比或有更强的依从关系时，把全部备份元件同时接入工作比当工作元件失效后再依次代换工作的方式可靠性高。

4. 其他技术

针对服务器硬盘和服务器的容错技术主要包括：

（1）双重文件分配表和目录表技术。

硬盘上的文件分配表和目录表存放着文件在硬盘上的位置和文件大小等信息，如果它们出现故障，数据就会丢失或误存到其他文件中。通过提供两份同样的文件分配表和目录表，把它们存放在不同的位置，一旦某份出现故障，系统将做出提示，从而达到容错的目的。

（2）快速磁盘检修技术。

这种方法是在把数据写入硬盘后，马上从硬盘中把刚写入的数据读出来与内存中的原始数据进行比较。如果出现错误，则利用在硬盘内开设的一个被称为“热定位重定区”的区，将硬盘坏区记录下来，并将已确定的在坏区中的数据用原始数据写入热定位重定

区上。

(3) 磁盘镜像技术。

磁盘镜像是在同一存储通道上装有成对的两个磁盘驱动器,分别驱动原盘和副盘,两个盘串行交替工作,当原盘发生故障时,副盘仍旧正常工作,从而保证了数据的正确性。

(4) 双工磁盘技术。

它是在网络系统上建立起两套同样的且同步工作的文件服务器,如果其中一个出现故障,另一个将立即自动投入系统,接替发生故障的文件服务器的全部工作。

9.5.3 容错系统工作过程

1. 容错系统经历的工作阶段

容错系统容许系统出错,但不会因故障而导致系统中断或出现错误。为了克服故障的影响,一个容错系统可能经历多达如下 10 个阶段。

(1) 故障检测:大多数失效最终导致产生逻辑故障。有许多方法可用来检测逻辑故障,如奇偶校验、一致性校验和协议违章都可以用来检测故障。故障检测技术有两个主要的类别,即脱机检测和联机检测,脱机检测时设备不能进行有用的工作;联机检测具有实时检测能力,检测与有用的工作可以同时执行。联机检测技术包括奇偶校验和冗余校验等。

(2) 故障限制:当故障出现时,希望限制其影响范围。故障限制是把故障效应的传播限制到一个区域内,从而防止污染其他区域。

(3) 故障屏蔽:故障屏蔽技术把失效效应掩盖了起来,从某种意义上说,是冗余信息战胜了错误信息,多数表决冗余设计就属于故障屏蔽。

(4) 重试:在许多场合,对一个操作系统的第二次试验可能是成功的,对不引起物理破坏的瞬间故障尤其如此。

(5) 诊断:对故障检测技术没有提供有关故障位置、性质的信息进行诊断。

(6) 重组:当检测出一个故障并判明是永久性故障时,重组系统的器件替换失效的器件或把失效的器件与系统的其他部分隔离开来,或使用冗余系统,确保系统能力不降低。

(7) 恢复:经检测和重组后,必须消除错误效应。通常,系统会回到故障检测前处理过程的某一点,并从这一点重新开始操作。这种恢复形式通常要后备文件、校验点和应用记录方法。

(8) 重启动:如果一个错误破坏的信息太多,或者系统没有设计恢复功能,那么恢复就不可能实现。仅当系统未受任何破坏时,才能进行"热"重启,并从故障检测点恢复所有的操作。"热"重启相当于系统需要完全重新加载。

(9) 修复:即把诊断为故障的器件还原下来,修复也可以是联机进行的或者脱机进行的。

(10) 重构:对元件进行物理替换之后,把修复的模块重新加入到该系统中。对联机修复来说,实现重构不中断系统的工作。

2. 容错系统工作过程

容错系统工作过程包括自动侦测、自动切换与自动恢复。

（1）自动侦测（auto-detect）。

运行中自动地通过专用的冗余侦测线路和软件判断系统运行情况，检测冗余系统各冗余单元是否存在故障（包括硬件单元或软件单元），发现可能的错误和故障，进行判断与分析。确认主机出错后，启动后备系统。

侦测程序需要检查主机硬件（处理器与外设部件）、主机网络、操作系统、数据库、重要应用程序、外部存储子系统（如磁盘阵列）等。

为了保证侦测的正确性，防止错误判断，系统可以设置安全侦测时间、侦测时间间隔、侦测次数等安全系数，通过冗余通信连线，收集并记录这些数据，作出分析处理。

（2）自动切换（auto-switch）。

当确认某一主机出错时，正常主机除了保证自身原来的任务继续运行外，将根据各种不同的容错后备模式，接管预先设定的后备作业程序，进行后续程序及服务。

系统的接管工作包括文件系统、数据库、系统环境（操作系统平台）、网络地址和应用程序等。

如果不能确定系统出错，容错监控中心通过与管理者交互，进行有效的处理，决定切换基础、条件、时延、断点。

（3）自动恢复（auto-recovery）。

故障主机被替换后，进行故障隔离，离线进行故障修复。修复后通过冗余通信线与正常主机连线，继而将原来的工作程序和磁盘上的数据自动切换回修复完成的主机上。这个自动完成的恢复过程用户可以预先设置，也可以设置为半自动或不恢复。

随着容错技术的研究深入与发展，容错系统开销会逐渐降低，纠错速度会更快，系统会更灵活，资源利用会更合理，检测与诊断将会采取人工智能的处理途径，以专家系统的各种智能工具来支持故障检测和诊断。系统的动态重构、故障恢复功能及神经元芯片等将被用到容错技术中来。

9.6 应用实例

9.6.1 运用 Norton Ghost 进行文件备份与还原

1. Norton Ghost 的功能

Norton Ghost 是美国赛门铁克公司旗下的一款出色的硬盘备份还原工具，可以实现 FAT16、FAT32、NTFS、OS2 等多种硬盘分区格式的分区及硬盘的备份还原。

Ghost 2003 可以在 Windows 环境下运行，但其核心的备份和恢复仍要在 DOS 下完成，Ghost 最新的版本是 15.0，可以让用户直接在 Windows 环境下，对系统分区进行热备份而无须关闭 Windows 系统，它新增的增量备份功能，可以将磁盘上新近变更的信息添加到原有的备份镜像文件中，不必再反复执行整盘备份的操作，它还可以在不启动 Windows 的情况下，通过光盘启动来完成分区的恢复操作。

2. Ghost 15 的安装与设置

（1）安装。

Ghost 15 的安装比较简单，可以在安装过程中选择需要安装的附加功能，Ghost 15 支持最新的 Windows 7 系统，并且在 Windows 7 中运行良好。目前下载的 Ghost 15 大都是英文的，但安装包里包含了简体中文版本，只需要解压安装文件，然后在 Install 文件夹里，运行 Setup. exe 就可以安装简体中文版的 Ghost 15。安装步骤如下：

① 运行 Setup. exe，然后在 Ghost 15 安装界面中单击【下一步】按钮，如图 9-8 所示。



图 9-8　Ghost 安装界面

② 在 Norton Ghost InstallShield Wizard 对话框中，勾中“我接受该许可证协议中的条款”，若要将 ghost 安装到 C 盘则单击【立即安装】按钮，若要将 ghost 安装到其他盘则单击【自定义安装】按钮，进行安装路径设置，如图 9-9 所示。



图 9-9　Norton Ghost InstallShield Wizard 对话框

③ 安装完毕重启计算机后，Ghost 15 有个激活向导，引导用户激活产品(不激活只可以免费试用 30 天)，在没有激活的状态下，用户可以正常使用 Ghost 15 的备份/恢复功能，但一些辅助功能不能使用。如果有密钥，选择第一个，输入许可证密钥并单击【下一步】按钮进行激活，如图 9-10 所示。

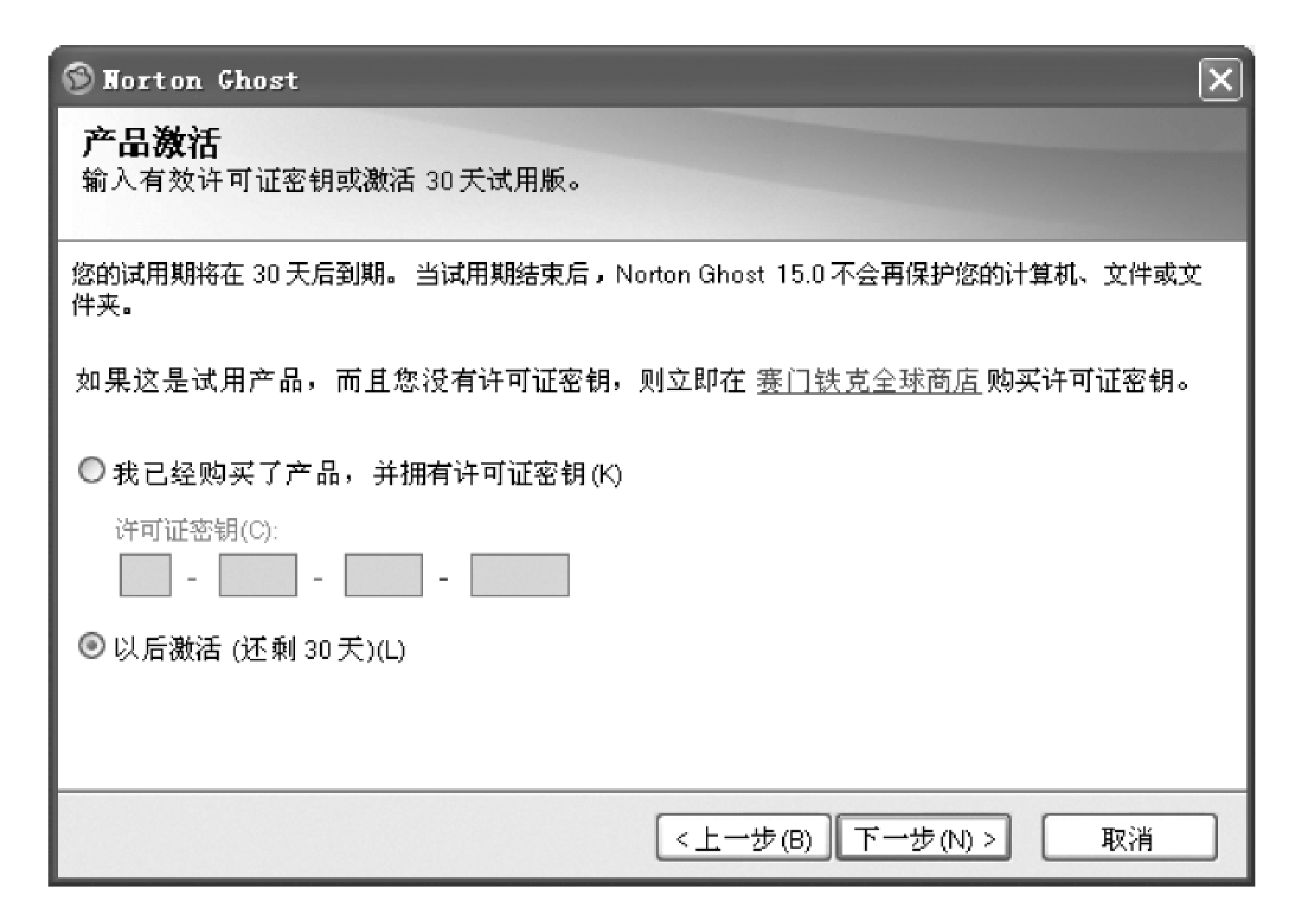


图 9-10　Norton Ghost 产品激活对话框

④ 进入完成界面，单击【完成】按钮。此时，要运行 Ghost 需要进行重启，在确保重要文件都已保存的情况下重启计算机，如图 9-11 所示。



图 9-11　Norton Ghost 安装完成对话框

(2) 初始设置。

为方便用户 Ghost 15 准备了一个“自动备份向导”，引导用户进行首次备份及进行相关的自动备份设置。用户可以对“备份计算机”(针对硬盘整个分区)与“备份‘我的文档’”(针对目录)进行设置，如图 9-12 所示。

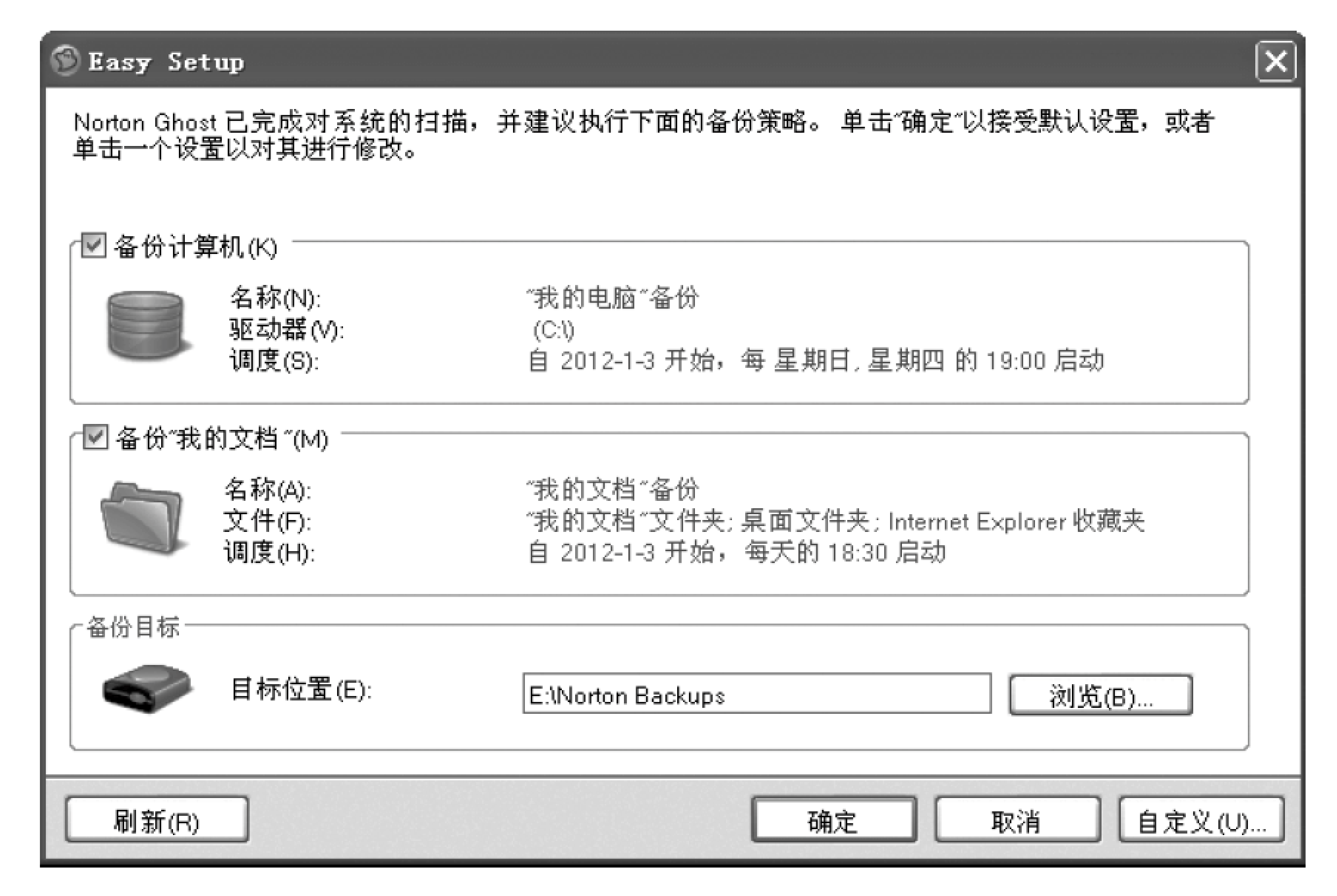


图 9-12　Easy Setup 对话框

设置的选项包括需要备份的目标、自动备份时间、自动备份激活条件、备份文件存储位置，以及多样的备份触发器。

① 设置备份的目标位置：在“Easy Setup”对话框的“备份目标”框中单击【浏览】按钮，可以选择备份存放的位置。

② 更改调度：在“备份‘我的文档’”框中单击“调度”命令，打开“更改调度”对话框，在这里可以指定运行备份的时间和频率，如图 9-13 所示。



图 9-13　“更改调度”对话框

③ 通过对事件触发器中的常规选项设置，可以指定在某些事件发生时自动运行备份，如图 9-14 所示。例如启动指定的应用程序或任意用户登录到计算机时运行备份，可以有效防止因操作失误而造成的损失或破坏，也可以有效防止黑客或病毒的攻击，通过恢复备份将应用程序或计算机状态恢复到黑客或病毒攻击之前的状态。

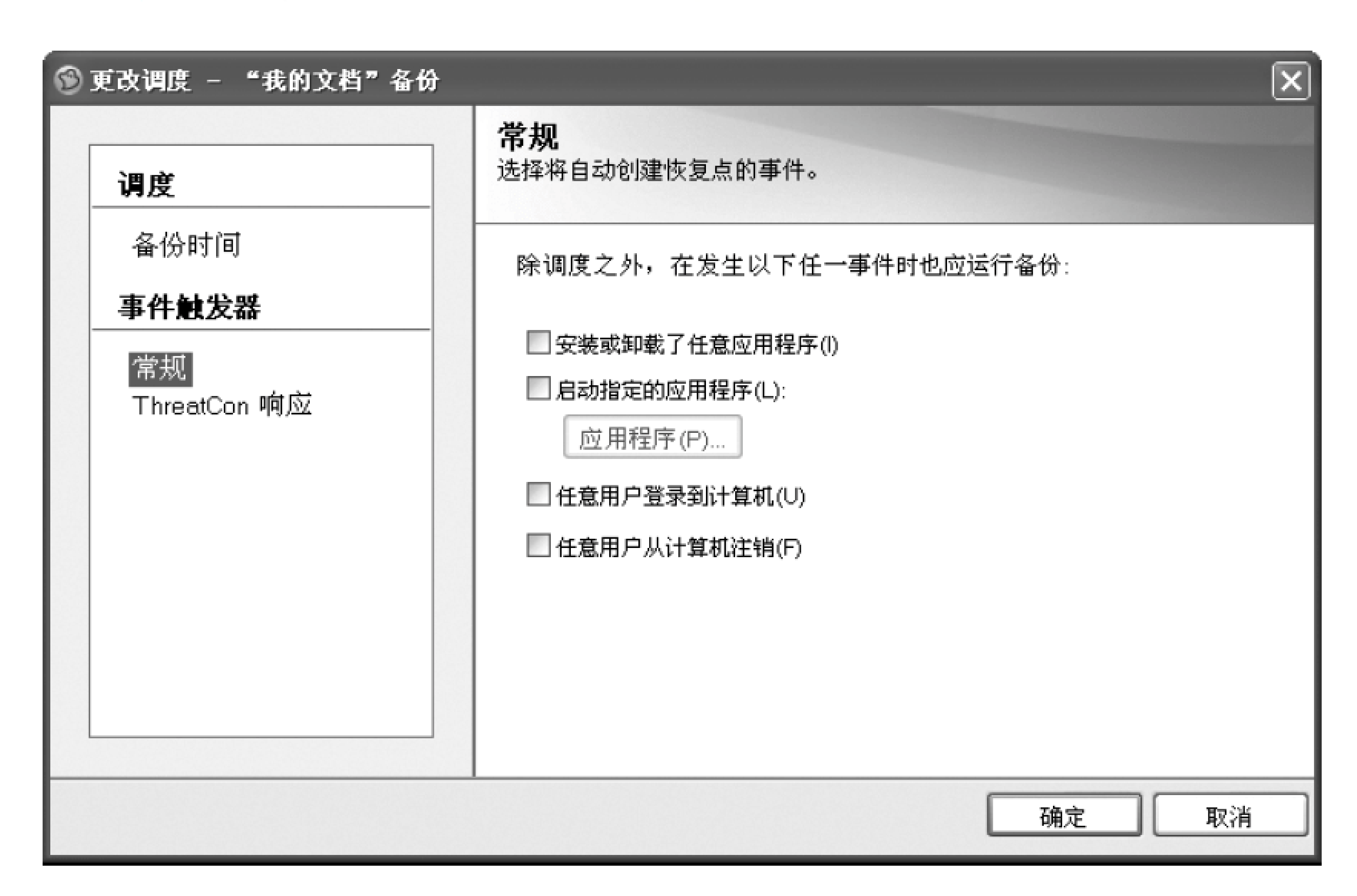


图 9-14　设置"常规"选项

（3）定义备份向导。

Ghost 15 为用户提供了更加详细的"定义备份向导"功能，用户可以通过它来一步一步地进行备份设置，步骤如下：

① 在"定义备份向导"对话框中选择"备份我的电脑"，单击【下一步】按钮，如图 9-15 所示。



图 9-15　"定义备份向导"对话框

② 在“备份驱动器选择”栏中选择 C 盘进行备份，单击【下一步】按钮，如图 9-16 所示。如果用户的操作系统安装不是安装在 C 盘(即系统引导数据在 C 盘而系统却非安装在C 盘)，当用户选择备份目标为系统所在分区时，Ghost 15 会自动提示用户同时备份引导数据所在分区，以免出现恢复系统后出现无法引导的问题。

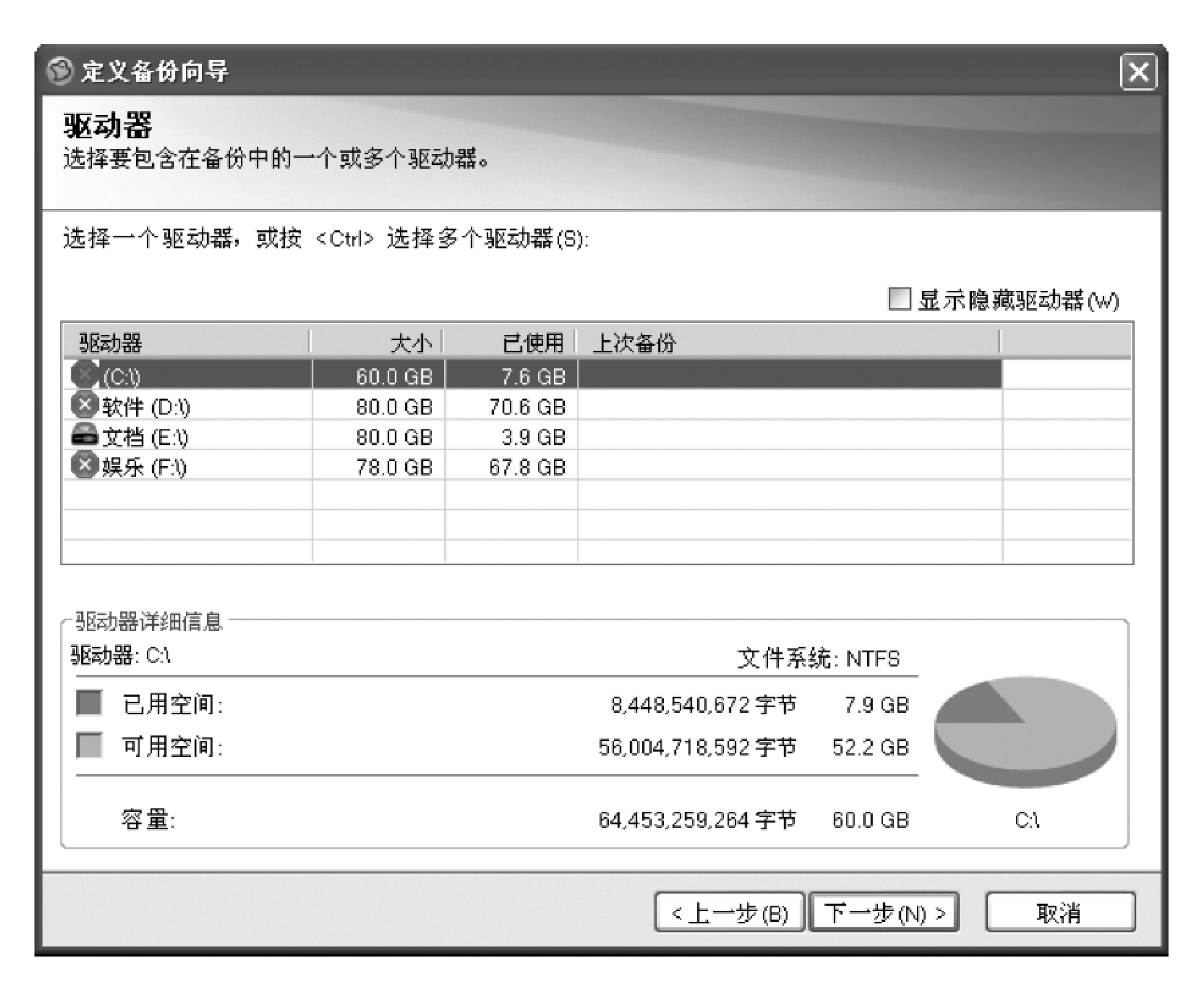


图 9-16　备份驱动器选择对话框

③ 选择“恢复点集”选项(恢复点集只备份变化数据，独立恢复点备份整个目标)，以节约备份所占磁盘空间及花费时间，如图 9-17 所示。

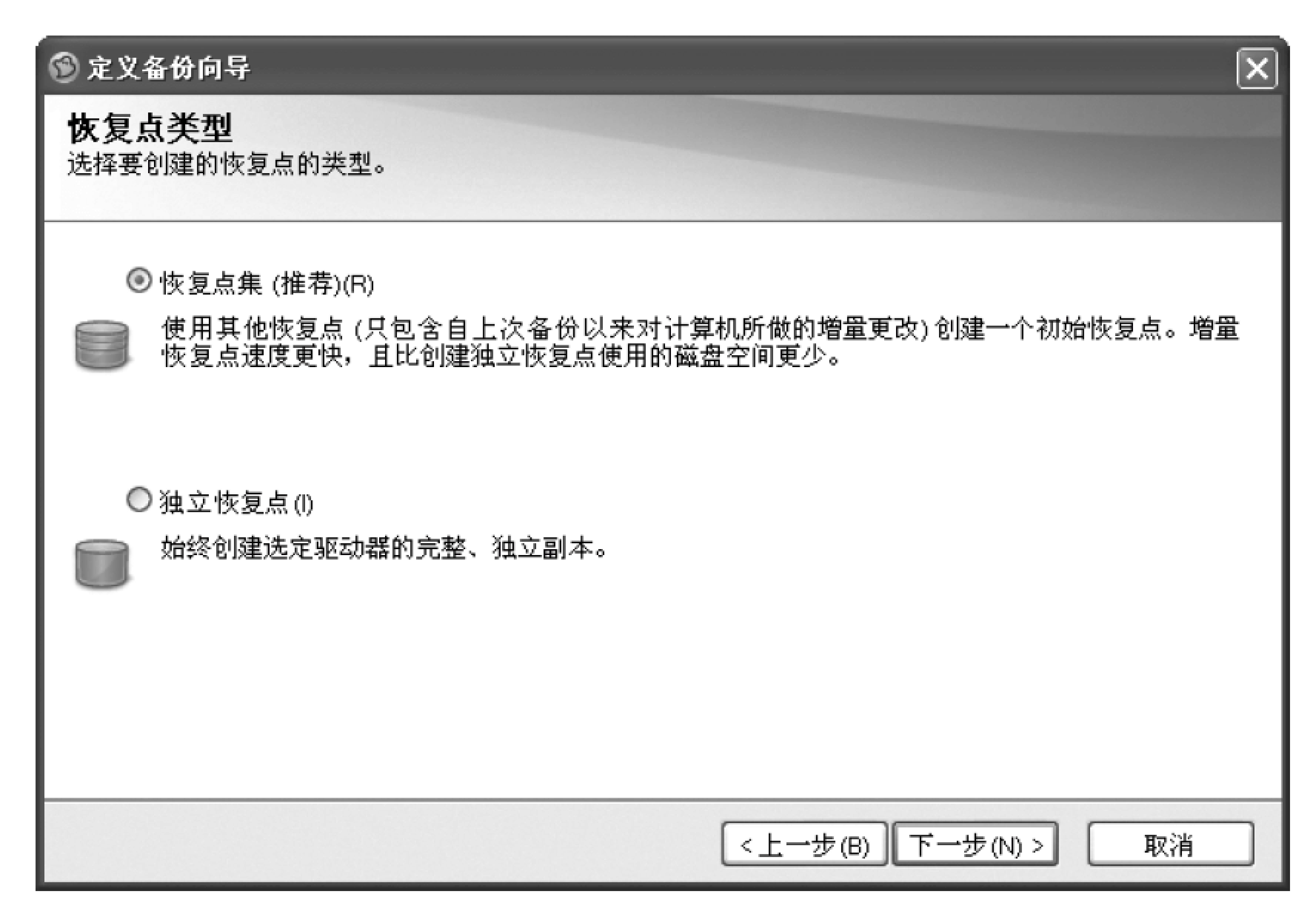


图 9-17　选择“恢复点集”选项

④ 用户除了将备份文件储存在本地磁盘空间外，还可以设置存储目录为备份目标。这样就可以避免本地硬盘出故障时，原文件与备份文件同时丢失的问题，如图 9-18 所示。



图 9-18　备份目标

⑤ 对于使用 Google Desktop 工具的用户，可以选中“为 Google Desktop 启用搜索引擎支持”，开启该功能后，用户就可以使用 Google Desktop 来搜索并恢复存储在恢复文件中的文件，如图 9-19 所示。



图 9-19　为 Google Desktop 启用搜索引擎支持

⑥ 用户可以选择对备份文件进行加密，Ghost 15 支持多种高强度加密方式，避免了备份文件泄密问题，如图 9-20 所示。



图 9-20　加密设置

⑦ 在备份时间中，根据自己的需要，设置备份时间和频率，如图 9-21 所示。



图 9-21　备份时间设置

⑧ 检验定义备份向导完成界面中的设置信息是否与你期望的设置一致，若一致，则单击【完成】按钮，若不一致，单击【上一步】按钮进行修改，如图 9-22 所示。



图 9-22 “定义备份向导”完成界面

当然备份整个磁盘分区这样的目标毕竟比较大，有时候系统是无关紧要的，最重要的还是用户的资料文件，没有必要为了备份某个文件而备份整个磁盘分区，那样未免太浪费备份空间与时间了。

在 Ghost 15 中用户在图 9-15 中选择“备份选定的文件和文件夹”选项即可。

3. 在 Windows 界面中运行 Ghost 15

(1) 进入 Ghost 15 的主页。

打开 Ghost 15 主界面选择“主页”标签，在这里用户可以看到当前的备份状态，备份目标状况，查看实时的赛门铁克的 ThreatCon 安全风险级别等信息，如图 9-23 所示。在任务栏里可以进行备份与恢复工作，其操作过程与前面的设置类似。

(2) 查看状态信息并恢复文件。

① 在 Ghost 15 主界面选择“状态”标签，可以看到备份情况状态表格图，如图 9-24 所示。可以看到各个磁盘分区的备份情况与备份时间，还可以快速地进行恢复操作。用户选中某个备份目标时，可以进行快速的文件或分区的恢复操作。例如，右击选择“恢复我的文件”命令。

② 在“恢复文件”对话框中输入部分文件名或者文件类型，例如输入“exe”，如图 9-25 所示。

③ 单击【搜索】按钮后，找到 3 个 exe 相关的文件，选中需要恢复的文件可以进行恢复，如图 9-26 所示。恢复文件时会显示文件恢复进程。



图 9-23　Ghost 主页



图 9-24　Ghost 状态界面

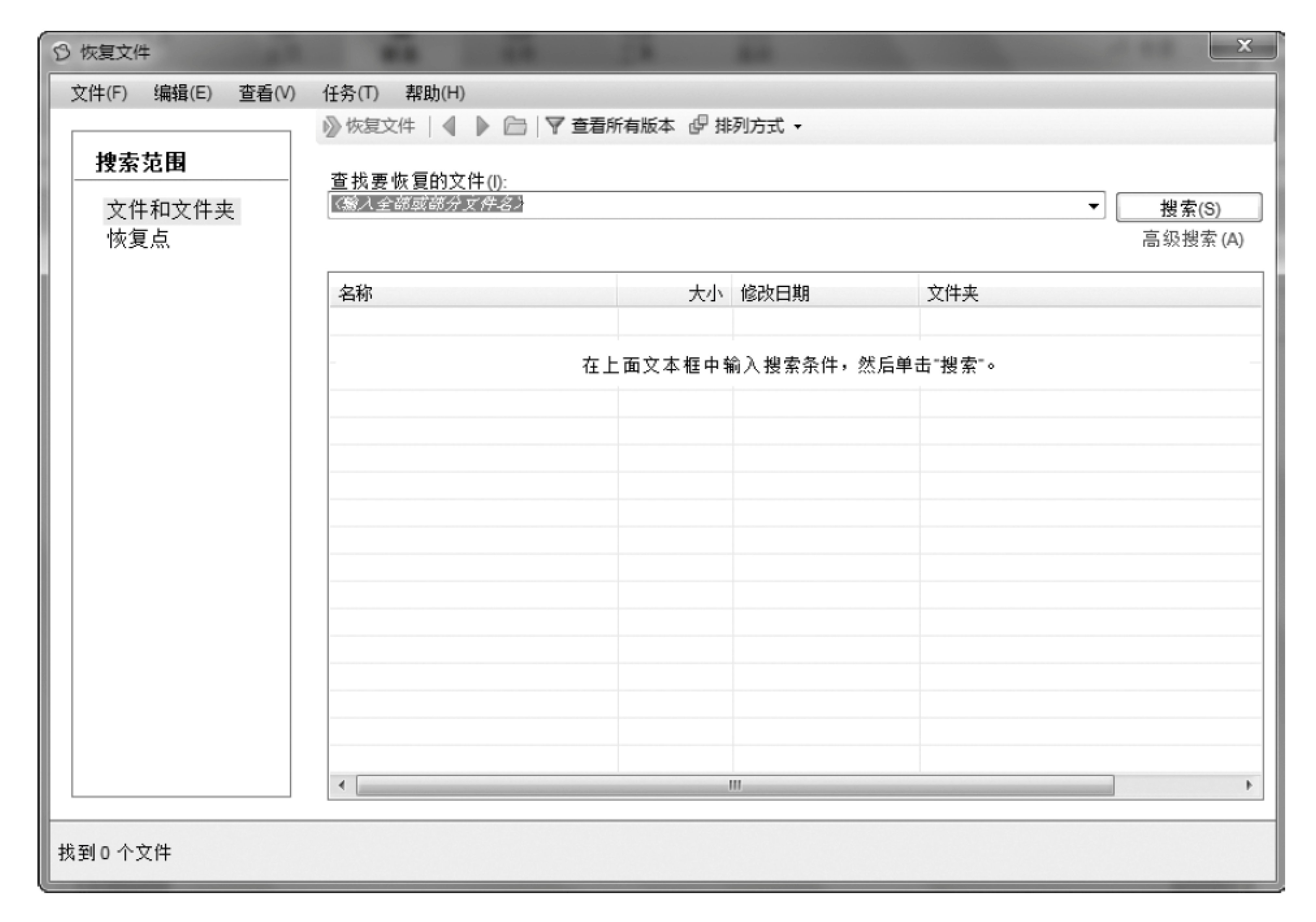


图 9-25 “恢复文件”对话框



图 9-26 选中要恢复的文件

4. Ghost 15 在系统崩溃下的还原

上面的操作可以在 Windows 系统下进行，但在计算机无法进入 Windows 系统时，该如何进行还原操作呢？操作步骤如下：

（1）用户需要使用 Symantec Recovery Disk CD 来引导启动，进入“恢复环境”后，在没有还原任务的前提下，会默认进入 Ghost 15 的 Windows PE 操作界面，在此用户只需选择“Home→Recover My Computer”菜单命令，打开 Recover My Computer Wizard 对话框，如图 9-27 所示，就可以进行分区或文件的还原操作了。

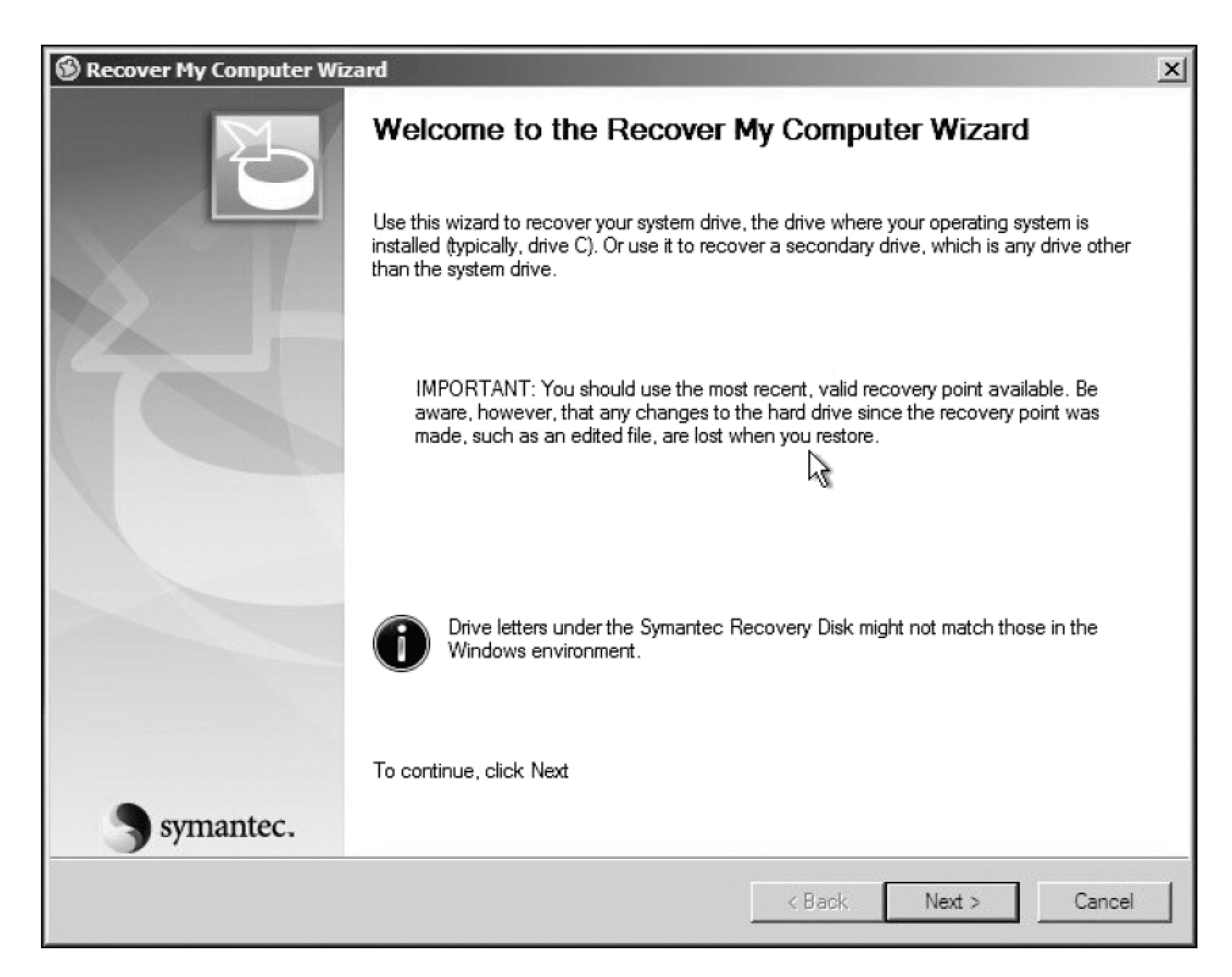


图 9-27　Recover My Computer Wizard 对话框

（2）单击【Next】按钮后，在图 9-28 中选择要恢复的数据备份。

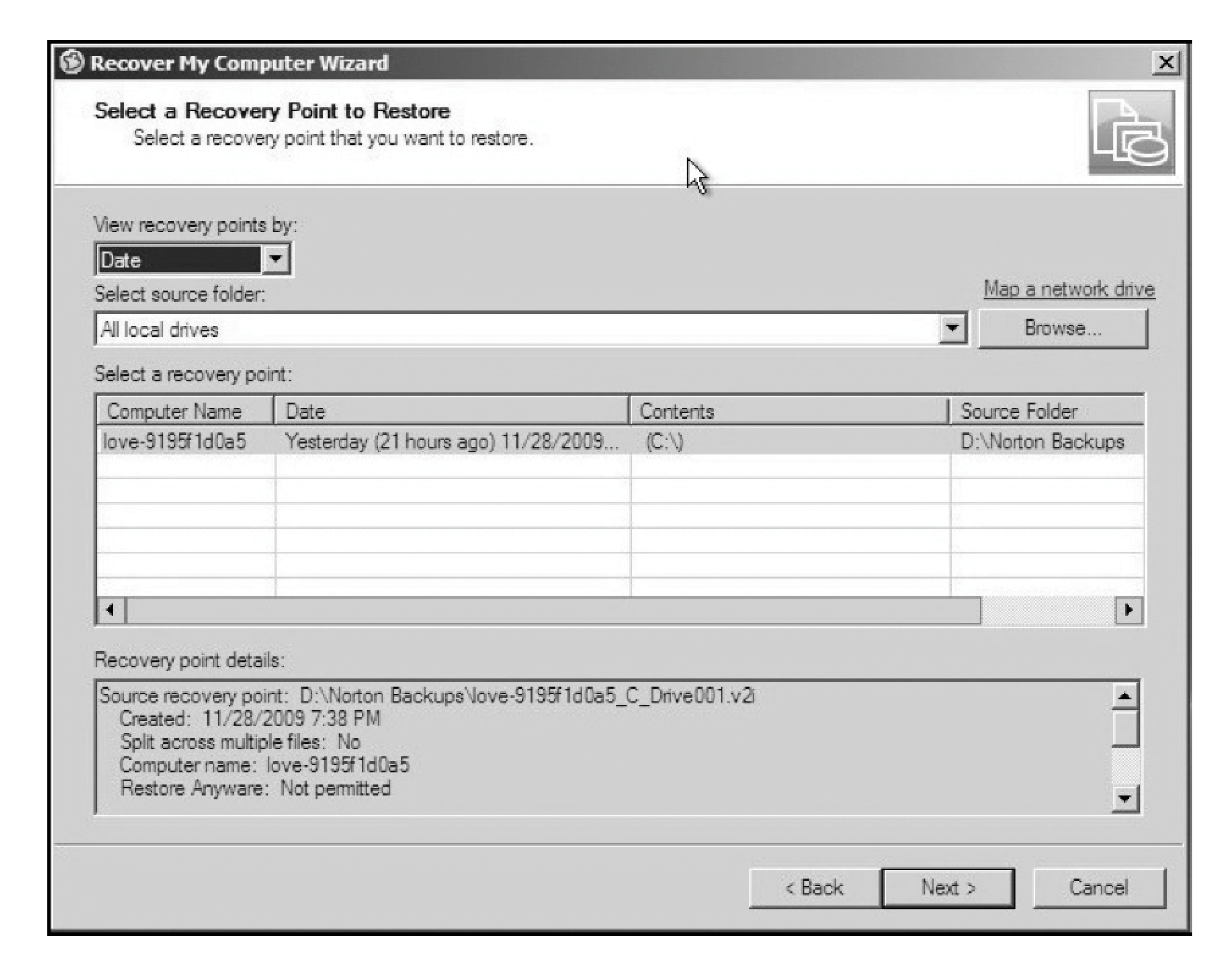


图 9-28　选择要恢复的备份

（3）单击【Next】按钮后，在图 9-29 中选择要还原到的位置，通常 C 盘为系统盘，这里选择 C 盘。

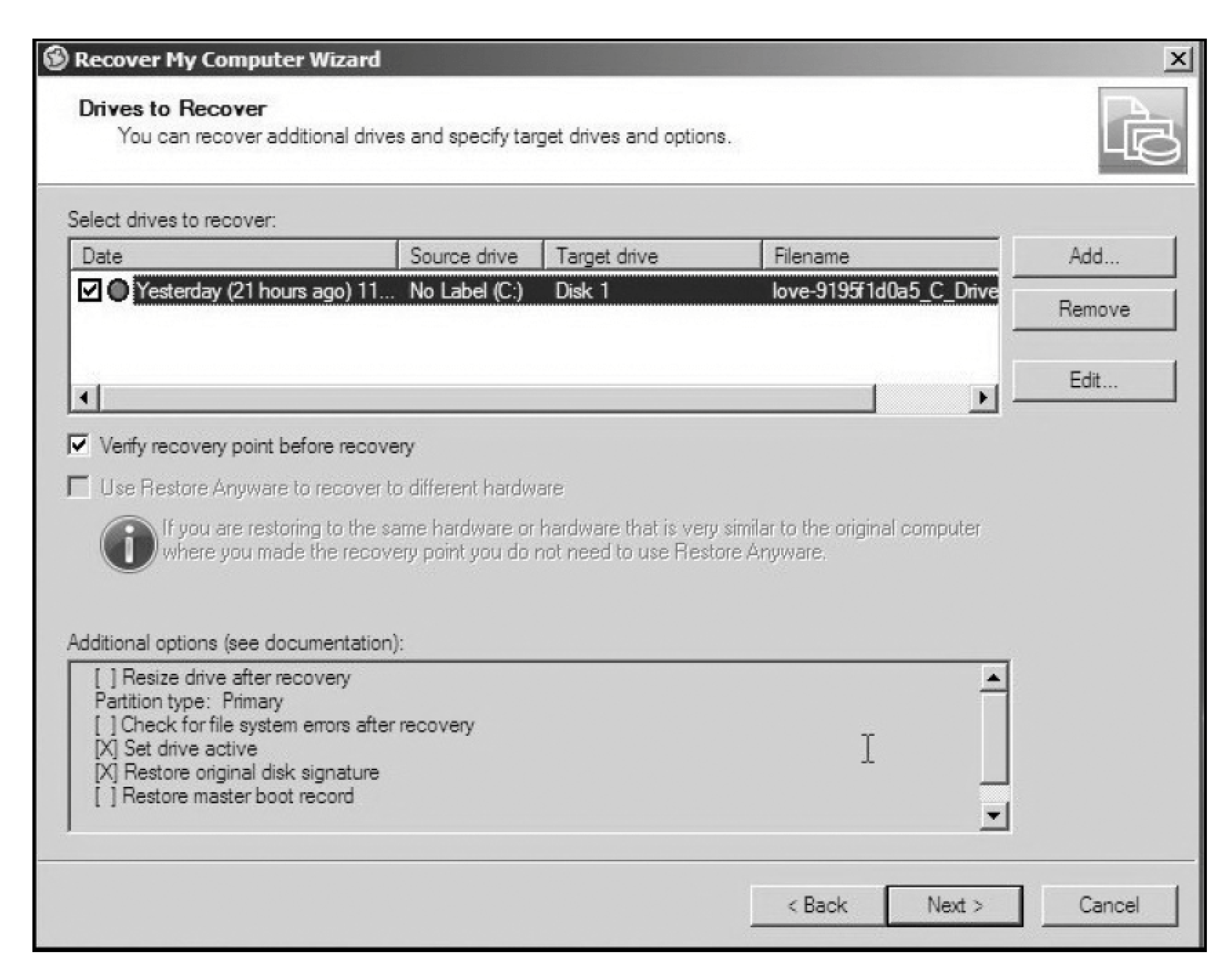


图 9-29　选择要恢复到的位置

（4）单击【Next】按钮后，在图 9-30 中确认恢复信息正确之后，单击【Finish】按钮。

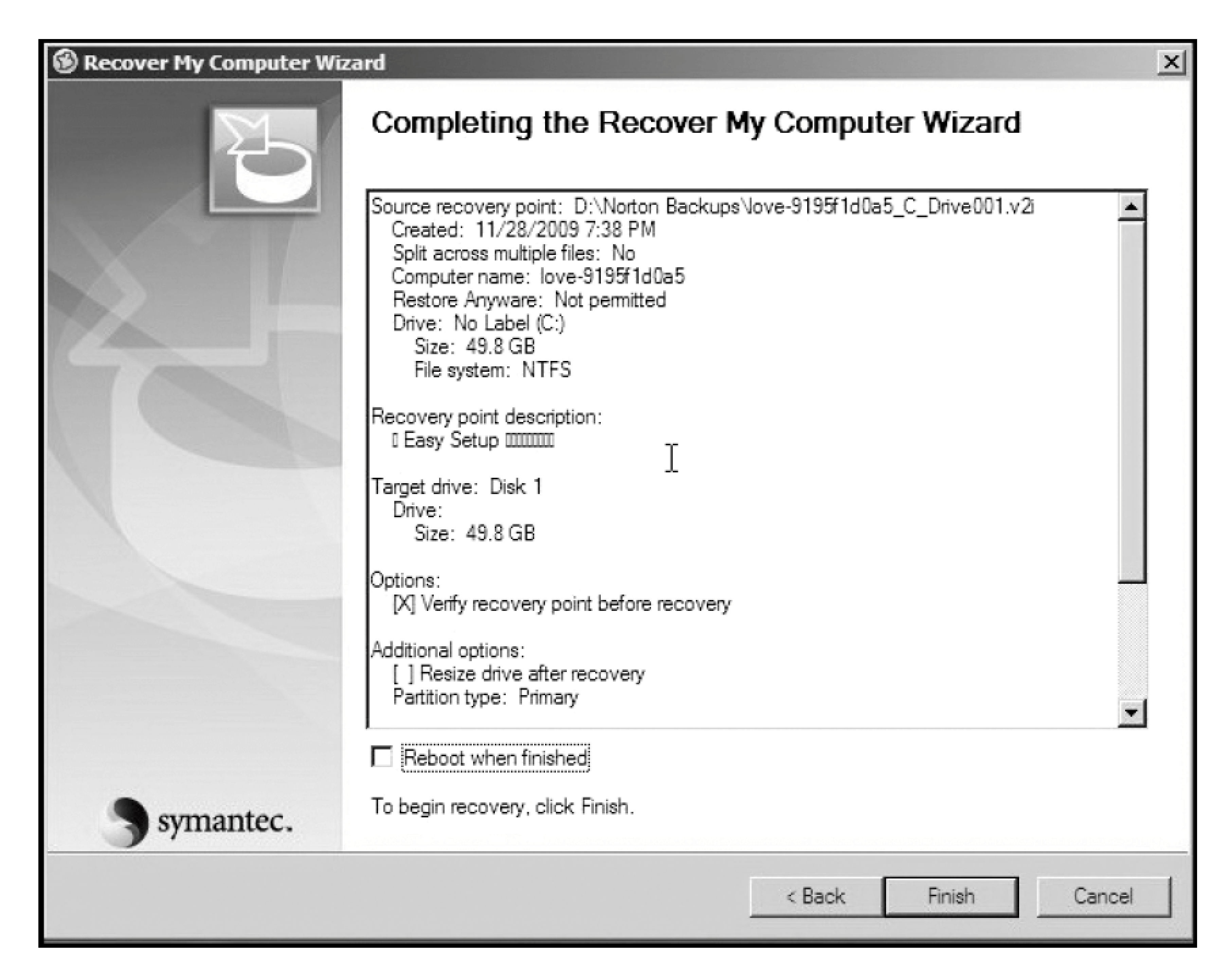


图 9-30　完成界面

9.6.2 运用 Windows 7 创建系统映像

在 Windows 7 中创建系统映像非常方便，操作步骤如下：

（1）在开始菜单中选择“所有程序→维护→备份和还原”菜单命令，打开“备份和还原”界面，如图 9-31 所示，可以在左侧看到“创建系统映像”菜单，单击菜单即可打开“创建系统镜像”对话框，如图 9-32 所示。



图 9-31　备份和还原

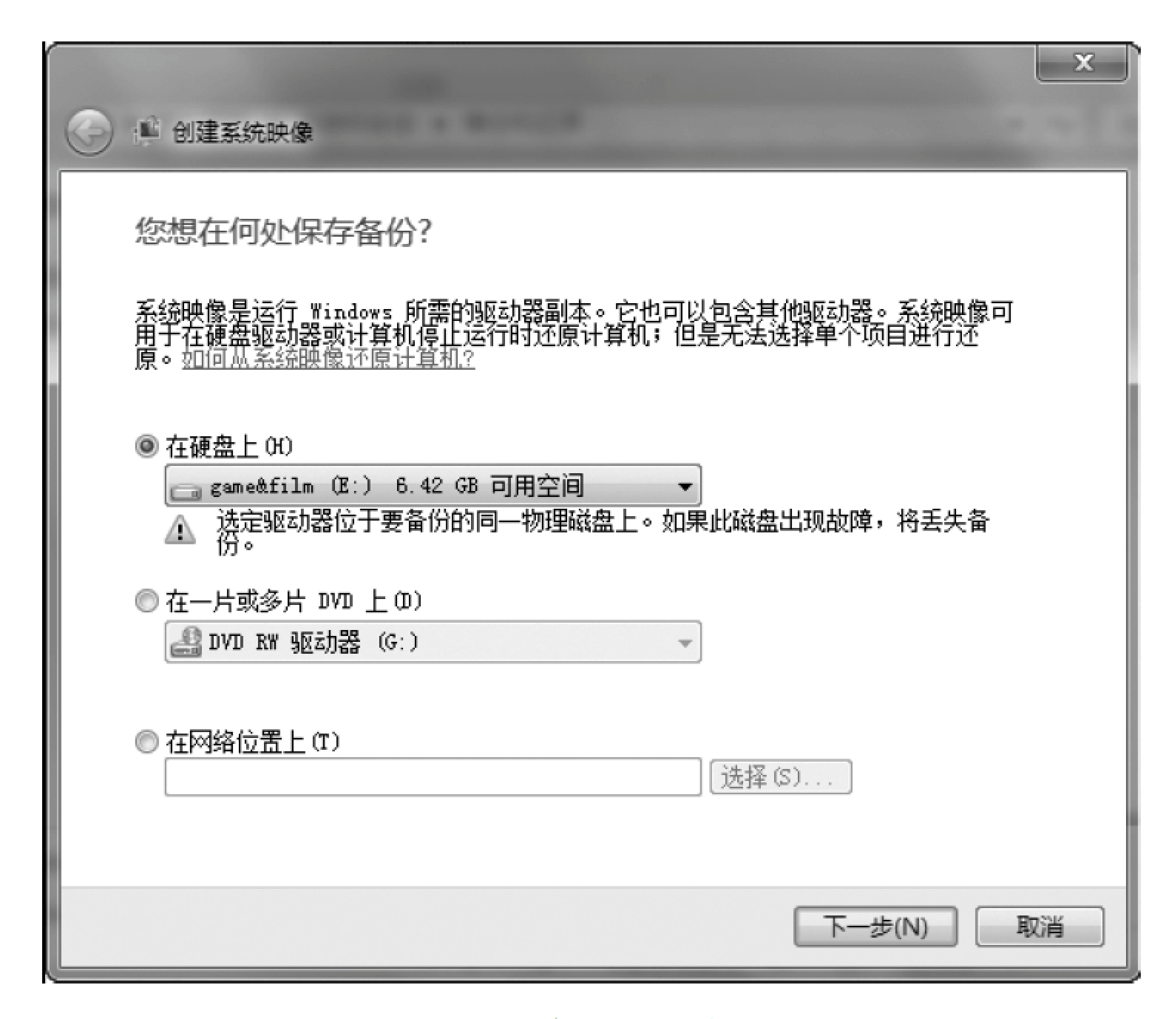


图 9-32　“创建系统映像”对话框

（2）在“创建系统映像”对话框中选定备份位置，如图 9-32 所示。单击【下一步】按

钮，后将开始备份，进程如图 9-33 所示。



图 9-33　备份进程

9.7　案例讨论

2004 年 12 月，冬天阴霾覆盖下的美国南部某州。狂风呼啸下，一栋高层楼房因电路短路突然起火，火势在风势下迅速扩大，成为熊熊燃烧的大火。这栋高楼的拥有者为一家州级商业银行。该银行的主数据中心及其管理人员均位于这栋起火的大楼里。主数据中心在这来势凶猛的大火下尽遭损毁。该中心里面的 90 台服务器和与之相连的存储设备、数据和应用软件均告毁坏并进而瘫痪。而建筑本身完全被毁。另外，这场火灾还造成一名系统管理员丧生，数名其他人员受伤。

火灾发生后，银行数据中心负责人来到 1.5 英里外的备份中心，打电话启动灾难恢复计划。幸运的是，银行新的灾难恢复计划的初始阶段在火灾发生前的 3 个月就已经开始实施。此外，在 6 个星期前，还进行了一场演练，因此每个人都对自己的角色记忆犹新。遗憾的是该灾难恢复计划副本保存在电子邮件文件中，而这些文件在火灾中丢失了。更为糟糕的是没有人打印过该计划，包括该计划的作者。因此，在从磁带中恢复电子邮件之前，系统管理员只能凭记忆进行灾难恢复。

恢复步骤由打电话构成。这些电话打往厂商、供应商、客户和用户。整个过程都按预定步骤的“人工脚本”进行，恢复计划中包含的所有应用都签有 SLA（service level agreement，服务级别协议），其中包括 2 小时的应用恢复点目标 RPO。这些签订的协议都得到了满足，没有丢失 45 分钟以上的任何电子事务处理，有数种应用根本什么也没有丢失。因为进入该公司计算机的每个事务处理都记录在纸上，最终没有丢失事务处理数据。

银行对于在这种规模的灾难中的所有关键应用事先都作了规划，计划中指定的恢复

时间目标 RTO 为 48 小时。所有应用都留有备份，这些备份在火灾后 48 小时内需恢复运行。应用快速恢复的一个主要原因是数据被异步复制到位于内不拉施加的奥马哈市的恢复站点。位于弗吉尼亚州备份站点的管理员挽救了所有关键数据，并使它们在奥马哈恢复站点重新上线。在恢复过程中，管理员使用了网络连接和拨号两种上网方式。虽然非关键应用的数据没有得到复制，但在恢复站点从备份磁带将这些数据恢复到了其他系统。

第一批恢复的信息服务在火灾后大约 24 小时恢复在线，所有应用的恢复则用了大约 10 天时间。灾难恢复计划没有预先确定恢复顺序，因此信息服务是按照特定用户的即时需求进行恢复。在发生冲突时，管理层就做出公断，根据业务关键性确定恢复的优先顺序。同时，管理层还进行了各种思想工作，让用户理解这种情况，即需要恢复的服务太多，而银行又没有足够的管理员来同时恢复它们。

从几个方面看，银行的灾难恢复总体上都是成功的。首先是灾难恢复计划所发挥的作用与预期一致。不同小组成员知道自己扮演的角色并像计划中所列的那样发挥自己的作用。所有备份与恢复、集群和数据复制软件的执行都与预期完全一致。但是，正如在这种规模的事件中可以预料的一样，有些事情的进展并非一帆风顺。例如，该公司备份数据的编目本身没有妥当备份，致使在进行了两天的读取磁带以重建编目工作后，一名管理员才记起某个恢复系统上有一份编目并找到和恢复了它。虽然编目恢复有些延迟，但也节省了几天的编目重建时间。

恢复过程中出现的其次一个问题是磁带机的缺乏，造成整个恢复过程的资源竞争。虽然利用适当规划，常常可以对应用的备份窗口进行分段，以最大限度地减少必需的磁带机数量，但是在这种所有信息服务数据同时被毁的灾难中，加快恢复进程的唯一方法就是使用更多的磁带机同时恢复更多的服务。

恢复中出现的另外一个问题是许多条码标签经磨损和撕扯后已脱落或毁坏。这样，许多备份磁带集因无法辨认变得不完整，从而无法得到恢复。因此，管理员只得从更早的备份磁带集中恢复系统。

另外，谁也没想到这场灾难的影响范围会有这么大。该公司的管理层一直以为在灾后较短时间内就能进入自己的办公大楼。他们虽预料到长时间电网故障和小规模火灾，但对引起数据中心长时间无法访问的灾难却无任何防备。幸运的是，该银行的信息技术供应商乐于提供帮助，如提供了现场和电话支持，增加了硬件、软件和许可协议序列号。

该公司经过如此重大灾难，对前期工作进行了反思。其重新设计了数据中心的几种运行方式。他们在信息处理中最重大的改变是在备份方面：如对备份编目进行远程复制和本地复制，对包含备份编目的磁带做了特殊标记。最重要的是，该公司购买了更多磁带硬件以提高将来的灾难恢复速度。由于火灾完全毁坏了原来的主数据中心，恢复站点的总部数据中心就成了永久性中心。灾难过后的另一个改变是灾难恢复计划从双站点（主站点和恢复站点）计划变为三站点计划：即用于运营和数据中心的主站点，以及位于远处的组合恢复站点。

另外，该公司利用这个机会将 90 台服务器上的应用整合到 10 台新的服务器中，并用存储网络将其连接成一个大型磁盘框架。对整合过的服务器做了 OS 升级，可支持多个运营区域。系统管理员则利用这种功能来实施本地集群和故障切换。结果是整个公司对

系统管理员有了一种感激之情，管理人员对恢复工作的迅速反应和有效管理使信息服务用户对他们更加尊敬。但最为关键的是所有人员都认识到灾难恢复的重要性。

你认为这家商业银行在灾难恢复过程中有哪些经验与教训？

你所知道的系统遇到过什么灾难吗？他们是如何进行灾难恢复的？

归纳总结

1. 分析归纳系统运行中面临哪些威胁。如何能避免这些威胁？
2. 归纳总结企业日常运营中应如何进行应急响应工作、灾难恢复工作与容灾工作。
3. 归纳总结企业进行应急响应、灾难恢复与容灾工作的工作流程。

思考与实践

思考题

1. 什么是应急响应？应急响应操作流程包括哪些内容？
2. 灾难恢复有哪些指标与等级？如何做灾难恢复需求分析？
3. 有哪些灾难恢复资源？什么是灾难恢复策略？可以采取什么灾难恢复策略？
4. 为什么要进行容灾建设？如何制订容灾计划？容灾与灾难恢复是什么关系？
5. 容错系统有什么作用？有什么特点？
6. 容错技术包含哪些主要技术？
7. 数据恢复的软件有哪些，这些软件分别有什么作用？

实践题

1. 在计算机上安装 Ghost，对系统和重要文件分别进行立即备份和定时备份，并尝试进行系统或文件备份的还原操作。

2. 在 Windows 7 操作系统下，使用 Windows 7 中自带的备份功能对系统和重要文件进行备份，并尝试进行系统和文件还原。

3. 使用 Winhex 软件进行硬盘数据删除与恢复练习。

参 考 文 献

1. 徐津,胡晓菲,潘威.计算机使用安全与防护.北京:电子工业出版社,2011
2. 安德森. 信息安全工程(第 2 版).北京:清华大学出版社,2012
3. 石勇,卢浩,黄继军. 计算机网络安全教程.北京:清华大学出版社,2012
4. 斯托林斯. 网络安全基础:应用与标准(第 4 版).北京:清华大学出版社,2012
5. 曹天杰. 计算机系统安全(第二版).北京:高等教育出版社,2007
6. 杨永川,黄淑华,魏春光. 边用边学网络安全技术.北京:机械工业出版社,2010
7. 翁正科. 计算机维护技术(第 5 版). 北京:清华大学出版社,2009
8. 王昭,袁春. 信息安全原理与应用. 北京:电子工业出版社,2010
9. 张同光,张有为,张家平等. 计算机安全技术. 北京:清华大学出版社,2010
10. 陈越. 数据库安全.北京:国防工业出版社,2011
11. 林果园.操作系统安全.北京:北京邮电大学出版社,2010
12. 徐茂智,游林. 信息安全与密码学.北京:清华大学出版社,2007
13. 陈鲁生,沈世镒. 现代密码学(第二版).北京:科学出版社,2008
14. 吴强. 加密与解密. 北京:企业管理出版社,2009
15. 武新华,安向东,刘国丽. 计算机安全技术. 北京:清华大学出版社,2000
16. 刘荫铭,李金海,范文庆,钮心忻. 软件漏洞的攻击与防范[J]. 电信科学. 2009,2
17. 陈敏. 软件加密技术与解密技术[J]. 软件导刊. 2007,6
18. 任海翔,吴茵. 软件安全保护:加壳与脱壳[J].网络安全技术与应用.2006,9
19. 许奎. 软件保护技术及其应用研究[D]. 安徽:合肥工业大学,2009
20. 谭貌,陈义,涂杰. 软件版权保护技术的研究与分析[J]. 计算机应用与软件,2007
21. 杨文虎,李飞飞.网络安全技术与实训(第 2 版). 北京:人民邮电出版社,2011
22. 吴多胜,王杰,王帆. 网络安全从入门到精通. 北京:电子工业出版社,2008
23. 郑秋生.网络安全技术及应用. 北京:电子工业出版社,2009
24. 刘化君. 网络安全技术. 北京:机械工业出版社,2010
25. 潘瑜. 计算机网络安全技术. 北京:科学出版社,2007
26. 张蒲生. 网络安全应用技术. 北京:电子工业出版社,2008
27. 张仁斌,李钢,侯整风. 计算机病毒与反病毒技术. 北京:清华大学出版社,2006
28. 刘功申. 计算机病毒及其防范技术. 北京:清华大学出版社,2011
29. 贾铁军. 网络安全管理及实用技术. 北京:机械工业出版社,2010
30. 陈月波. 网络信息安全(第 2 版). 武汉:武汉理工大学出版社,2009
31. 安葳鹏,刘沛骞.网络信息安全.北京:清华大学出版社,2010
32. 刘化君.网络安全技术.北京:机械工业出版社,2010
33. 杜晔,梁颖.网络信息对抗.北京:北京邮电大学出版社,2011
34. 袁津生,吴砚农.计算机网络安全基础(修订本).北京:人民邮电出版社,2004
35. 牛少彰. 信息安全导论. 北京:国防工业出版社,2010
36. 刘洪发、唐宏. 网络存储与灾难恢复技术. 北京:电子工业出版社,2008
37. 李飞,陈艾东,王敏. 信息安全理论与技术. 西安:西安电子科技大学出版社,2010
38. 邹恒明.有备无患:信息系统之灾难应对.北京:机械工业出版社,2009